12-2015

Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know

Casey J. Gordon
University of Nebraska-Lincoln, kcwags@yahoo.com

ADDRESSING SECURITY RISKS FOR MOBILE DEVICES: WHAT HIGHER EDUCATION LEADERS SHOULD KNOW

by

Casey J. Gordon

A DISSERTATION

Presented to the Faculty of

The Graduate College at the University of Nebraska

In Partial Fulfillment of Requirements

For the Degree of Doctor of Philosophy

Major: Education Studies

(Educational Leadership and Higher Education)

Under the Supervision of Professor Miles Bryant

Lincoln, Nebraska

December, 2015

ADDRESSING SECURITY RISKS FOR MOBILE DEVICES: WHAT HIGHER EDUCATION LEADERS SHOULD KNOW

Casey J. Gordon, Ph.D.

University of Nebraska, 2015

Adviser: Miles Bryant

This qualitative study examined the topic of mobile device security at higher education institutions in the Midwestern United States. This study sought to answer the question of how higher education institutions have responded to threats to campus data security posed by mobile devices. It explored the questions of what institutions are doing currently, the policies and procedures they have in place, and what leaders should do in the future.

This research study consisted of four case studies, compiled through interviews with key Information Technology (IT) professionals and faculty at each of the four institutions studied as well as an examination of the web sites of each institution.

Themes from the research included:

- Frequent communication with faculty, staff, and students is absolutely critical to the success of security initiatives.
- The creation of a security awareness program and security policies are critical to mitigating the highest risk area, which is the end users themselves.
- Institutions lack the resources, both financial and staffing, to handle these growing needs.

- There is a high need to balance access with security to ensure that the mission of higher education can still be completed.
- As the variety of devices grows, it is critical to protect the data at the source rather than try to control the device itself.
- Three of the four institutions studied had newly created or newly restructured Chief Information Security Officer roles.

Recommendations for future research included studying the changing dynamics of how mobile devices are used for education specifically, exploring various ways to move the emphasis of security from the device to the data itself. Research should also narrowly focus on the particular issues of passcode usage among faculty, staff, and students, as well as studying what makes a successful security awareness program. It is also necessary to examine actual security breaches that have occurred at higher education institutions and what qualities are needed in a successful Chief Information Security Officer (CISO) position.

DEDICATION

To my mom and dad.

For teaching me to never give up.

For teaching me how to work hard.

For teaching me to leave things in better shape than I found them.

For teaching me to always see the best in people.

For believing in me.

ACKNOWLEDGEMENTS

Thank you to my husband, Aaron Gordon, for listening to my research problems, encouraging me to keep going, and watching our kids, Zach and Spencer, so that I could complete this project. Thank you to my entire family for all of the time they spent taking care of and entertaining my children so that I could write. Mom (Linda), Dad (Richard), Jeanna, Kristi, Mike, Pat, Kayla, Cole, Ashley, and Hailey, I couldn't have done this without you all supporting me and helping me. A special thank you to Jeanna for sharing her valuable time and expertise with me.

Thank you to my advisor, Dr. Miles Bryant, for his guidance and insights, as well as his willingness to stick with me despite the fact that I took an incredibly long time to finish this project. Many thanks to my committee for their helpful advice and feedback which enabled me to greatly improve the finished product of this research study.

Thank you to Phil Thorson for mentoring me for the last ten years and always helping me see a different perspective. Thank you to Thad Wakefield for providing that extra nudge whenever my motivation was waning.

Thank you to all of my interview subjects (you know who you are) and readers for your time and expertise. The wealth of knowledge that is housed within each of you is vast, and I am incredibly honored for the time you bestowed upon me.

TABLE OF CONTENTS

CHAPTER 1 – INTRODUCTION

Statement of the Problem

Many higher education administrators believe that security is an extremely important strategic challenge facing their institutions today, and the massive growth of mobile devices has provided a new kind of security risk. Educause, a nonprofit association whose mission is to advance higher education by promoting the intelligent use of information technology, conducts a yearly survey of their membership, and security ranked in the top three concerns from 2007 through 2010 (Agee, Yang, & Educause Current Issues Committee, 2009; Allison, DeBlois, & Educause Current Issues Committee, 2008; Camp, DeBlois, & Educause Current Issues Committee, 2007; Ingerman, Yang, & Educause Current Issues Committee, 2010). In 2013, this Educause survey revealed that the number one concern of participating institutions was "Leveraging the wireless and device explosion on campus" and the number five concern was around information security and developing an appropriate balance between openness and security (Grajek & 2012-2013 Educause IT Issues Panel, 2013).

As the Bring Your Own Device (BYOD), Bring Your Own Technology (BYOT), Bring Your Own Applications (BYOA), or Bring Your Own Everything (BYOE) phenomena grow in popularity among higher education institutions (French, Guo, & Shim, 2014), the question of how to protect institutional data continues to be a major focus for institutions. Mobile devices, once seen as an add-on in the educational environment, are now essential to daily activities (Elahi & Islam, 2014; Imgraben, Engelbrecht, & Choo, 2014; Miller, Voas, & Hurlburt, 2012; Thomson, 2012; Wankel & Blessinger, 2012). In 2015, the yearly Educause survey stated that the number seven

concern of participating institutions was “Providing user support in the new normal - mobile, online education, cloud, and BYOD environments,” closely followed by the number eight concern which was “Developing mobile, cloud, and digital security policies that work for most of the institutional community” (Grajek & 2014-2015 Educause IT Issues Panel, 2015, p.14). Whereas earlier surveys discussed simply the idea of security and the need to “respond to regulatory compliance mandates” (Grajek & 2013-2014 Educause IT Issues Panel, 2014, p.12), the most recent 2015 survey has evolved to emphasize that security is not simply about locking down access and information but must be a balance that allows the educational community to reach their goals while still protecting institutional data.

Despite the fact that security has been a major focus for higher education institutions for many years, the area of mobile devices is still a major challenge. In an interview with Zumerle (2015), he stated:

> The reality is that the threats targeting mobile devices have not changed. There are still two main causes of data loss on mobile devices: physical device loss and misuse of apps. What has changed is the severity of the consequences. Mobile devices are now storing and accessing more-sensitive data. In healthcare, for example, an increasing number of physicians are using tablets to process sensitive data about their patients. In finance, brokers are using their smartphones to exchange sensitive information. In these scenarios, a device that falls in the wrong hands and does not have adequate protection can be the source of a major data breach.

Higher education institutions often have financial, healthcare, and many other types of private data that faculty and staff are accessing in a variety of ways. Because of this, many leaders need guidance as to the security risks surrounding mobile devices and how to address these various types of security risks at their institutions. The mobile device has become the most common IT device in everyday life and a likely target for theft and security breaches (Clarke & Furnell, 2005; Mahesh & Hooter, 2013). Mobile devices, because of their portability and smaller size, are subject to greater threat of theft than other types of devices which remain safely on campus, locked in offices (Botha, Furnell, & Clarke, 2009; Mahesh & Hooter, 2013; Miller, Voas, & Hurlburt, 2012). Because of their connection to the Internet through various unsecured methods, the varied security of apps, and the fact that users can access nearly all of the same information that was previously only accessed from protected desktop computers, mobile devices are subject to risk of security breaches as well (Botha, Furnell, & Clarke, 2009). Higher education administrators must be aware of and prepared to address the risks associated with these devices. Miller, Voas, and Hurlburt (2012) state that:

> Given exposure to technology from early consciousness, it's hard to envision a workplace of the future that won't involve BYOT—the "digital natives" will demand it. BYOT is already common in many businesses. (p.54)

If leaders do not prepare their higher education institutions to address this growing population, they will be leaving information and data, some of which is confidential, subject to theft and data breach. Furthermore, they will risk negative publicity and potential lawsuits from constituents whose private data have been exposed (Educause, 2014).

While past research has explored mobile device usage or the security of mobile devices, there is a deficiency in that little time has been spent examining mobile device security specifically at the location of higher education institutions. Faculty and staff in higher education may be using these devices for very different purposes than those in the private sector. Those uses may include research and exploration, and the culture of higher education is often thought of as a more open environment than that of the private sector. Because universities often have less control over the types of devices their employees and students use than private sector businesses, this can create unique challenges, and it is important that researchers study this location specifically to determine the implications in this particular setting. Mobile devices utilized in higher education institutions might be owned by the institution or personally-owned, making it more difficult to enforce controls and policies. Several examples of the ways in which mobile devices are being used in higher education are provided later in the chapter.

While security issues at higher education institutions have also received much research attention, there has been little focus specifically on the area of mobile devices relating to security. Therefore, the topic of mobile device security and how it affects higher education institutions in particular bears further investigation. This study attempted to remedy these deficiencies because it sought to explore mobile device policies and procedures at higher education institutions as well as how these institutions are currently addressing mobile device security. By creating a holistic picture of what the University is doing today to handle mobile device security, this research study begins to highlight areas of need that institutions should address and areas of strength that can be built upon for the future.

The purpose of this qualitative research study was to explore how four-year higher education institutions in the Midwestern United States have been addressing the variety of issues that accompany mobile devices. This study sought to explore the security issues around mobile devices that are facing higher education institutions today and how the leaders of those higher education institutions can prepare their institutions to handle these issues tomorrow. Additionally, this study sought to answer the question as to how leaders can continue to address mobile device and data security issues in ways that are sustainable into the future. The intended audience of this paper is higher education administrators, IT department leaders, IT security professionals, and others interested in IT security issues in higher education. This study sought to assist this audience in preparing their institutions to handle mobile device security for their faculty, staff, and student populations.

Research Questions

The overall research question that this study sought to answer is:

- How have four higher education institutions responded to the threats to campus data security posed by mobile devices?

In addition, the author formulated four key sub-questions:

- How are the selected higher education institutions in the Midwestern United States addressing mobile device security today?
- What policies and procedures surrounding mobile devices have the selected universities established?
- How are the selected institutions balancing the question of security versus accessibility and usability?

- In what ways can leaders proactively handle security challenges that will be brought on by mobile devices in the future?

Research Objectives

The objectives of this research were to explore the security risks facing higher education institutions regarding the usage of mobile devices and how institutions are addressing these security risks. This research also sought to understand the policies, procedures, and best practices in existence that can assist in supporting mobile devices. A third objective of this research study was to determine how higher education institutions can prepare their institutions to protect themselves from risks associated with mobile devices in the future.

Background Information

In a survey conducted by the Association for Information Communications Technology Professionals in Higher Education (ACUTA) in 2009, researchers found that 84 percent of respondents believed their campus networks were more secure than five years ago (Worldwide Videotex, 2009). Yet, despite those findings, 47 percent of respondents had experienced a significant security breach at their institution of employment. Researchers also found that 35 percent of respondents saw mobile devices as the most vulnerable area. Other top vulnerabilities included internal controls, student downloads, student hackers, and Internet access. Fifty-eight percent of respondents stated that they are currently dealing with security by attempting to educate their students and staff, and 44 percent stated that they were tightening internal controls and addressing problems through implementing new systems.

Gartner (2010) published a report which stated that it is critical that businesses closely manage their mobile devices because of their increasing popularity. Gartner stated that all mobile devices have security risks and "that mobile devices have access to more private data and can expose more about user activity and actions than any other component in the user's technology arsenal" (p. 3). Because mobile devices track location information, payment information (example: Apple Pay), and much more, they often contain even more personal data than a laptop or desktop computer. However, more recent research indicates that the movement to BYOD makes it nearly impossible to closely manage mobile devices. The floodgates are open, and data are being accessed from everywhere using every different kind of device imaginable (Thomson, 2012). Cisco security expert Gordon Thomson (2012) states that "A willingness to balance risks and benefits is a hallmark of IT's new posture toward security. Instead of outright bans on devices or access to social media, enterprises must exchange flexibility for controls with which workers can agree" (p.5). In a study conducted by CDW-G (2009) about federal government cyber security, researchers found that risks around mobile computing are increasing at a more rapid rate than other types of risks. Data assets held by educational institutions are varied, and it can be a large challenge to institutions to ensure the protection of all of these systems through all possible methods of access (Custer, 2010). Control over mobile devices is no longer an attainable goal.

Definition of Terms

Acceptable Use Policy: sometimes referred to as an AUP. In higher education, a set of rules outlined by the institution that dictates how the network, website, computers, e-mail, and other institutional resources may be used by the end user. For example, this

policy may restrict the personal use of institutionally-owned devices, may prevent end users from downloading unsupported software to institutionally-owned devices, or may prevent institutionally-owned devices and resources from being used for personal profit.

Architecture: often used to refer to systems architecture or security architecture. This term refers to the technology specifications, models, and guidelines that assist in designing a system. This can be thought of as simply the framework or design that makes up the system or security infrastructure.

Attacker: in the world of cyber security, a person that attempts to destroy, expose, disable, steal, or gain unauthorized access to an institution's data or systems.

Bio-authentication: also called biometric authentication. This uses a person's physical characteristics to grant access into a system or service. Typical usages of this include fingerprint, retina scanning, or facial recognition to unlock a device or open a door.

Bluetooth: a type of wireless technology for exchanging data over short distances. This type of technology is typically used to connect devices together. For example, it can connect a keyboard and mouse to a computer wirelessly. For the purposes of this study, this refers to mobile devices which use Bluetooth to connect to other mobile devices, to create Wi-Fi hotspots to which other mobile devices can connect, and to connect to speakers and other peripherals.

BYOD: stands for Bring Your Own Device. Bring Your Own Technology (BYOT), Bring Your Own Applications (BYOA), or Bring Your Own Everything (BYOE) are all different variations of the same idea, referring to the trend of the student,

employee, or person bringing their own technology to utilize instead of the institution providing it.

CISO: stands for Chief Information Security Officer. This is an individual charged with handling IT security at an institution. Some institutions will have different versions of this position, such as an Information Security Officer (ISO) or a Security Manager. This position may fall under an IT department's purview, but it also may report directly to the President, finance area, or risk management area.

Cloud: sometimes called "cloud computing" or "cloud storage." This is a trendy term for online services and storage. This means that the cloud is essentially a network of remote systems presented over the Internet and used to store, manage, and process data instead of housing that information locally on an institution's own computers and systems.

Confidential Data: also called private data. This term is used to describe data that are non-public in nature. This may include student records, such as grades, e-mail addresses, mailing addresses, and phone numbers. It may also include social security numbers, banking information, and other non-public data.

Cyber Hygiene: refers to steps that computer users can take to improve their cybersecurity and better protect themselves online.

Cybersecurity: being protected against the criminal or unauthorized use of electronic data.

Data Classification: in the field of security, categorizing types of data in order to determine how secure that data needs to be kept. For example, this ranges from public

data which can be unsecured to confidential data which needs to be more secured. Often HIPAA data are classified as restricted data, which requires the highest level of security.

Dark Reading: a website, a subsidiary of InformationWeek, dedicated to reporting technology security issues and vulnerabilities. http://www.darkreading.com/

Data plan: wireless technology that refers to smartphones and tablets which connect to cellular networks and transmit data over their network, paid monthly for a certain amount of data or an unlimited amount. This type of wireless technology is typically thought to be more secure that traditional Wi-Fi.

DHS: stands for Department of Homeland Security. http://www.dhs.gov/

DMCA: stands for Digital Millennium Copyright Act. This is a United States copyright law. In higher education, institutions are provided notices from the DMCA that outline details of any violation of the Copyright Act, along with identifying information about the type of device that was used to commit the illegal act. This enables institutions to track down the violator and take action to remove the content.

End users: people who utilize mobile devices. For the purposes of this study, this refers to faculty, staff, students, and other constituents of higher education institutions.

Exfiltrating: the unauthorized transfer of data from a computer.

Exploit: a piece of software, some amount of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause harm to computer systems.

Extreme Case Sampling: the process of selecting or searching for unusual cases of the phenomenon of interest. In the case of this study, the researcher sought institutions that were leaders in the area of IT in order to provide insights on what institutions in that leading position were doing around mobile device security.

FERPA: stands for the Family Educational Rights and Privacy Act. This is the Federal law that protects the privacy of student educational records.

Gap Analysis: the comparison of actual performance with desired performance. In IT and security, this is the practice of assessing where weaknesses lie in the security infrastructure and determining the largest security risks for an organization.

Good Technology: a company that provides a mobile device management solution. There are many vendors in this marketplace, and this is just one example. https://www1.good.com/

HIPAA: stands for the Health Insurance Portability and Accountability Act. These are the federal regulations in place to protect the confidentiality and security of healthcare information. Higher Education institutions with health centers on campus, nursing programs, and counseling programs need to comply with these regulations.

HITECH: stands for the Health Information Technology for Economic and Clinical Health Act and is focused on the expansion of electronic health record systems across the United States. It also widens the scope of privacy and security protections available under HIPAA, as well as increases the liability if institutions do not comply.

Information Assurance: the practice of managing risks related to the use, processing, storage, and transmission of information or data and the systems and processes used for those purposes. Some institutions have an Information Assurance Policy that will be the procedure for managing these risks.

Infrastructure: the physical and organizational structures and facilities (e.g., hardware, cabling, power supplies, et cetera) needed for the operation of a computing environment.

Internet of Things: sometimes referred to as IoT. It describes the inter-connectedness of “things” embedded with electronics, specifically referring to an environment in which objects, animals, or people are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human interaction or human-to-computer interaction. An example of this would include Disney’s Magic Bands.

IT: information technology. This term is often used to encompass all aspects of technology, including computers, mobile devices, software, infrastructure, and more, often as it directly applies to the application of these technologies in the business sector

MaaS360: a company that provides a mobile device management solution. There are many vendors in this marketplace, and this is just one example. http://www.maas360.com/

Malware: malicious software that is intended to damage or disable computers or any system on which it is installed.

MMS: stands for Multimedia Messaging Service. It allows people to send messages that contain multimedia content to and from mobile phones, such as pictures and video. Typically this is through the normal text messaging feature on a smartphone.

Mobile Devices: portable electronic devices including laptops, smartphones, tablets, electronic readers, and other devices. For the purposes of this study, laptops are excluded because they are essentially managed similarly to desktops, and this research is focusing on other types of mobile devices, ranging from tablets to smartphones.

Mobile Device Management (MDM): sometimes called MDM or an MDM system. This is a system used for the administration of and protection of mobile devices,

including smartphones, tablets, and sometimes laptops and desktops as well. These systems can be used to keep track of inventory of the devices, force certain security policies (such as a passcode), and manage software and app licenses.

NIST Cybersecurity Framework: stands for National Institute of Standards and Technology and their division of cybersecurity in which they create a framework and roadmap for institutions to use as guidance regarding best practices around the security of instructional data and systems.

Passcode: in terms of mobile devices, a password used to gain entry to a mobile device, sometimes a series of numbers.

Password Manager: a software application that allows a user to store and organize passwords. The end user uses one “master password” that is extremely strong, and that gains access to their entire password database. This type of software typically will also generate and suggest secure and very strong passwords for end users to use for all of their accounts.

PCI: stands for the Payment Card Industry. This is a set of requirements to ensure that all companies secure credit card information correctly. These regulations set guidelines for how data can be processed, stored, and transmitted. Most higher education institutions have some amount of PCI data from merchants on campus to accepting credit cards to pay tuition.

PHI: stands for Protected Health Information. This is any information about health status, provision of health care, or payment for health care that can be linked to a specific individual.

Phishing: the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

REN-ISAC: stands for the Research and Education Network Information Sharing and Analysis Center. This is a community of members who work together to promote cybersecurity within the research and higher education communities.

Risk Assessment: a process to identify potential hazards or risks and analyze what could happen if a hazard or risk occurs.

RSA: RSA SecurID, a mechanism for performing two-factor authentication by assigning a random authentication code at fixed intervals to ensure the identity of the person logging in.

SANS Top 20 Critical Security Controls: sometimes called simply the “SANS Top 20” and refers to a set of twenty security controls. Security is a massive undertaking, so rather than provide an exhaustive list of every risk in an organization, the SANS Top 20 seeks to prioritize and focus on a smaller number of actionable controls with high payoff, aiming for a "must do first" philosophy. They were derived from the most common attacks and vetted across a very broad community of government and industry. Found here: https://www.sans.org/critical-security-controls/

Security Breach: any incident that results in unauthorized access of data, applications, networks, or devices by bypassing or “breaching” their security mechanisms.

Security Threat: in terms of technology, a possible danger that might exploit a vulnerability and cause a breach in security resulting in possible harm.

Spoofing: a situation in which one person or program successfully masquerades as another by falsifying data. An example of this may be an e-mail that looks like it comes from a legitimate source when, in reality, it is not truly coming from that e-mail address at all.

SMS: stands for Short Message Service. Quite simply, this is the technical term for text messaging.

Two-factor Authentication: also called 2FA or Multifactor Authentication. This is an added layer of security that requires both the typical username and password, as well as something extra to which only that user has access such as a PIN or a code that is texted to that user's cell phone number which is on file with the company.

VPN: stands for Virtual Private Network. A VPN connection extends a private network across a public network, such as the Internet, enabling a device to send and receive data across shared or public networks as if it were directly connected to the private network. For example, once a VPN connection is established with the on-campus network, even if the device is off-campus, it is subject to the same security rules as though it is on-campus.

Vulnerability: a weakness which allows an attacker to reduce a system's information assurance. There are typically three components to a vulnerability: a system susceptibility or flaw, an attacker having access to the flaw, and an attacker capability to exploit the flaw.

Wi-Fi: also called wireless. This is a local area wireless technology that allows devices to connect to and participate in computer networking. This technology uses either the 2.4 GHz or the 5 GHz radio bands.

Delimitations and Limitations

Delimitations and limitations assist in establishing boundaries for conducting a study. Delimitations include choices made by the researcher about what is and is not included in the study. This study does not focus on laptops, but on other types of mobile devices such as smartphones and tablets. Because most laptops contain a full operating system, they are typically managed similarly to desktop computers. This technology has been at institutions for many years, and most institutions have policies and procedures around supporting these types of devices already. The purpose of this study was to research the area of mobile devices that is newer and currently still lacking much of this policy and procedure, namely smartphones and tablets. Therefore, one delimitation of this study is that it will not examine laptops.

Another delimitation is that this study did not examine two-year higher education institutions nor any institutions outside of the Midwestern region of the United States. There are a vast number of differences in mobile devices, from the type of device to the usage of the devices. Because of the incredibly large scope of this topic, the researcher chose to narrow the focus to four-year higher education institutions in the Midwest.

One delimitation of the research study is that the researcher opted to ensure the anonymity of the institutions and the subjects. The researcher chose this because the topic of security is sensitive, and the researcher hoped that this would protect the institutions from any type of harm. However, because of this, the researcher was unable to provide

exact details about the institutions as a precaution in order to protect the source. In addition, the researcher was unable to present web links for the web sites and policies that the researcher utilized in the study in order to protect the identity of the subjects and their institutions.

A limitation is described as an influence on the researcher which is outside of the researcher's control (Baltimore County Public Schools, 2010). One limitation of this study is the institutions examined have differing styles of handling data and policies. Some institutions have this information readily accessible on the web sites, and others contain that information in an internal area that was unable to be accessed by the researcher. Because of this, there will be many policies and practices that are not able to be studied or described in this research. As a result, the researcher could not provide specific information as to exactly which individual policies each institution had created. Because of the vast variety of systems, digital information, and data, this is a limitation of the study.

An additional limitation of the study is around the willingness of the institutions and the participants to be studied. There were institutions and interview subjects who were reluctant to be studied because of the nature of the study which dealt with security. These difficulties obtaining research subjects are described in greater detail later in the study. Reasons that were cited by prospective interview subjects included a fear of causing harm to the reputation of their institution, as well as a fear of exposing too many details about their institution which could leave their institution vulnerable to an attack. Another reason cited frequently was that the potential interview subject felt that their knowledge was not deep enough in the subject of mobile device security to be of value to

the study. Interview subjects that did agree to be interviewed may still have been reluctant to disclose details about their institution out of fear of painting their institution in a negative light or exposing too much information which would put their institution at risk. The consequences to the study are that the researcher had to look for other institutions and other experts to interview, which could have impacted results.

Another limitation of this study is that mobile device security is a rapidly changing field, and new approaches to managing security are constantly being created. What is uncovered in the research today may be irrelevant in a few years as technology evolves. Because of the fast pace at which technology changes, this is an important limitation of this research study.

Significance of the Study

A 2011 Educause report states that "mobile devices amplify existing security concerns while introducing a new set of risks" (p.1). In order to protect private data, institutions must first understand the risks introduced by these devices. Institutional data assets are being accessed from a variety of devices, networks, and locations. The constant availability of institutional data is one of the things driving institutions forward, helping them reach their educational goals, but it is also what puts the institution at risk of data breach, loss of data, and legal action. Information technology security is not something that should only be dealt with after a breach occurs. Faculty, staff, and administrators need to understand the risks surrounding mobile devices in order to help prevent these security incidents from occurring in the future. Educause (2011) also reports that higher education institutions in particular face a unique set of risks regarding mobile devices, stating:

> Colleges and universities are the custodians of considerable amounts of sensitive information. Regulations such as HIPAA and FERPA hold institutions accountable for a wider range of data than many other organizations, and a litany of data breaches involving stolen laptops and misplaced flash drives chronicles higher education's spotty record with electronic data. Meanwhile, the explosion of mobile devices quickly erodes the control that institutions might otherwise have had in terms of software updates and patches on devices that access campus networks. Most mobile devices are purchased and maintained by individuals, whether students, faculty, staff, or other users who access campus networks. Measures to limit the amount of data stored on mobile devices and tools (such as remote-wiping applications) can mollify the risk, but the days of tight control have likely passed. (p.2)

The rapid proliferation of data being stored and accessed online has created a whole new area of expansion for higher educational institutions, bringing with it a new set of questions and complications. Data previously stored in paper files is now available to be accessed and used electronically in order to assist with decision-making. Who has access to digital information is a critical question facing higher education leaders today.

In higher education, there are many possible scenarios around mobile devices that may play out. For example, Professor A has an iPad Mini that she purchased with her professional development funds. She connects to wireless Internet wherever it is available for free. Yesterday, Professor A found a network in a local coffee shop called "Free Coffee Shop WiFi" and connected. While there, she checked her e-mail, submitted grades to her course management system, and checked her bank balance. She was none

the wiser that her “free” Internet connection was not provided by the coffee shop at all, but set up by a person nearby for the sole purpose of spying on and stealing the information of anyone connecting to it. University data have now been compromised, and the University is unaware of the security breach.

Staff Member B has a personal Android tablet that he sometimes uses for work purposes. The University makes him have so many different passwords, and they all have different rules about including numbers and letters. Professor B finds it confusing, so he has his tablet save all his passwords so that he doesn’t have to type them in each time. Staff Member B’s children also use the tablet around the house. Last night, his teenage daughter had friends over, and they were all looking up information on the Internet using the tablet. This morning, Staff Member B noticed that there were some files moved around and that his University e-mail was opened sometime last night. His e-mail contains many confidential files from students and professors he supports, as well as student grade information. University data have now been compromised.

Professor C has a smartphone that she purchased with her own money, and she bought the data plan so that she is able to use the Internet from anywhere with cellular reception. She has downloaded apps to use on the smartphone to access the University’s resources, such as Blackboard and e-mail. She also downloaded an app that says it will allow her to access her documents that she has stored on the University’s computer from her smartphone. She has typed in her University-issued username and password and has used the app several times to open up assignments from students that she has stored on her computer. She does not realize that this app is not from a reputable source, that the creator of the app is capturing the username and password she is submitting, and that the

creator of the app now has full access to any system that uses her University username and password. University data have now been compromised, and once again, the University is not aware of the breach.

Professor D has set up his own wireless network at home. He bought the router that was recommended at a local retail store, and when he plugged it in, his iPad was able to connect to it perfectly. However, what Professor D does not know is that his neighbor has been using his Internet connection as well to surf the web and watch Professor D's Internet activities. Lately, his neighbor has even started collecting the information that Professor D has been sending across the Internet such as his usernames and passwords. The neighbor now has the power to log into all of Professor D's University accounts, bank accounts, and personal accounts. University data have now been compromised, and the University is unaware of the breach.

Student E leaves her Bluetooth on all the time so that she can connect her smartphone to her Bluetooth speakers in her dorm room. When she enters the library, she is unaware that there is a hacker there scanning for phones with Bluetooth enabled, downloading her phone information and installing malware onto the phones that tracks the activity of the device. Student E logs into her University accounts, accesses her bank account, enters credit card information in a webpage, and registers for classes using her smartphone. The hacker captures all of this information and uses Student E's University login to gain access to the University network to begin an attack on University systems and data. University data have now been compromised, and the University is unaware of the breach.

These scenarios are happening today across the United States, and each of these scenarios could have been prevented. Yet what are universities doing today to prevent these types of incidents from occurring? If a data breach occurs, the ramifications to the institution can be vast, ranging from a small impact to a large impact on the institution. In a less severe scenario, the institution will need to notify those affected and modify their practices to ensure no further breach occurs. In a more severe scenario, the institution will also need to notify the parties affected, take steps to prevent future breaches, and even be subject to lawsuits from individuals whose data were compromised. A common practice today is also for institutions to pay for at least a year of credit monitoring for any affected parties. Coping with a security breach can often involve spending a great deal of money to bring in security specialists to analyze what happened and provide advice in how to prevent security issues in the future. According to Custer (2010), the average cost of cleanup after a data breach at an educational institution is $210,000 or higher. This can be an important justification for preventative measures. In many cases, the negative publicity surrounding a data breach may be even more detrimental to the institution than the actual data breach itself (Brechbuhl, Bruce, Dynes, and Johnson, 2010). Not only will the institution need to address what happened, but students, parents, alumni, and other constituents of the organization will lose trust in the institution. This trust is critical to the successful continued operation of the University.

CHAPTER 2 – LITERATURE REVIEW

Introduction

There is no single definition for what makes a mobile device "secure." Yet despite this lack of a definition, higher education institutions are constantly trying to make their environments more secure than they are today. Without a consistent definition, this can be a challenging task. Brechbuhl, Bruse, Dynes, and Johnson (2010) stated that security can be defined quite simply as risk management. When applied to mobile devices, higher education institutions are essentially attempting to reduce the risk to their organization that is incurred by using mobile devices. Risk cannot be eliminated entirely without severe ramifications to the environment (Thomson, 2012). A review of the literature demonstrated that there are a wide variety of risks that may need to be managed when dealing with data being accessed from mobile devices, and seeking to prioritize these risks can assist higher education institutions in addressing them. Managing these risks takes time, effort, and often reduces the freedom of a faculty or staff person to use their device. Institutions must weigh the risks and the benefits of implementing these security measures in order to achieve the appropriate balance of freedom and security. In order to do this, literature has demonstrated that there are several key areas in which leaders should focus their efforts.

How Mobile Device Security is Unique

First, it is important to consider how mobile security differs from conventional computer security. La Polla, Martinelli, and Sgandurra (2012) found that there are five main distinctions:

• *mobility*: each device comes with us anywhere we go and therefore, it can be easily stolen or physically tampered;

• *strong personalization*: usually, the owner of device is also its unique user;

• *strong connectivity*: a smartphone enables a user to send e-mails, to check her online banking account, to access a lot of Internet services; in this way, malware can infect the device, either through SMS or MMS or by exploiting the Internet connection;

• *technology convergence*: a single device combines different technologies: this may enable an attacker to exploit different routes to perform her attacks;

• *reduced capabilities*: even if smartphones are like pocket PCs, there are some characteristic features that lack on smartphones, e.g. a fully[sic] keyboard. (p.6)

Computing devices at large institutions and businesses are typically governed by administrative systems which control the software and set specific security rules and settings, often restricting end users from deviation from those standards. Many institutions have installed a Mobile Devices Management system, called an MDM (French, Guo, & Shim 2014). This allows institutions to lock down the mobile device, determine exactly what is allowed to be installed on the device, apply security and passcode rules, wipe the device, and enforce many other control-based features.

In the past year, experts have been shifting their advice, recognizing that mobile devices are not the same as computing devices and need unique attention and focus (French, Guo, & Shim, 2014). An Educause Executive Brief on information security released in August of 2014 states that:

> The increasing prevalence of the bring-your-own-everything (BYOE) phenomenon stresses the importance of sound information security practices. User-provisioned technologies are often seen as bigger security issues because institutions and their IT departments have little or no control over the devices that users introduce to the institutional network. Thus, security practices designed to protect data—as opposed to protecting the delivery mechanism—are important. Implementing and improving mobile security for data is a high or essential priority at 55% of institutions. (p.5-6)

This shift is important because it means that institutions need to focus on protecting the data so that confidential and private information is secure regardless of how and where it is being accessed.

In addition to the items listed above, there are several factors that make it extremely difficult to control mobile devices. These are the combination of institutionally-owned and personally-owned devices, the massive variation in makes and models of mobile devices, and the incredible pace that mobile devices change operating systems and hardware. Therefore, the new approach being recommended in the arena of security is that institutions focus on securing the devices to a certain extent, but also on securing the data so that institutional data are protected regardless of the method of access used (Educause, 2014). This allows institutions to better focus their resources to address the real risk; loss of institutional data.

Security Risks to Mobile Devices

In order to develop a comprehensive approach to mobile device security, one must understand each of the potential security risks associated with mobile devices.

Because of the resources it would take an institution to address all security risks, it may become necessary to focus an institution's efforts on the security risks that are the most prevalent and the most detrimental to higher education institutions. With so many threats facing mobile devices, it can be overwhelming for institutions to attempt to address all these risks. Friedman and Hoffman (2008) compiled a list of seven threats to mobile device security. Their research study consisted of examining research around mobile device usage, comparing and contrasting it with desktop and laptop computers, and using this research to determine the most prevalent mobile device security threats that existed at that time. They sought to understand the threats that were unique to mobile devices specifically, as opposed to desktop and laptop computers. The threats that they compiled were "malware, phishing and social engineering, direct attack by hackers, data communication interception and spoofing, loss and theft of devices, malicious insider actions, and user policy violations" (p.159).

Verma (2011) completed a research study which compiled a list of the top ten threats to smartphone security. Verma analyzed research and documentation around smartphone security, trends around smartphone usage, and how smartphones address those threats. In doing so, the author developed a list of the key threats including malware, data loss, loss and theft of the devices, insecure data transfer, and end user behavior. Research by Mahesh and Hooter (2013) supports this, finding that malware intrusion and data theft are large concerns in the arena of mobile device support. Mahesh and Hooter's research reviewed "corporate policies posted on websites along with research papers and corporate whitepapers to develop a comprehensive user owned mobile computing device policy" (p. 2).

End users as the largest risk.

Recent research indicates that end users themselves are woefully unaware or unconcerned with the risks associated with mobile device usage. Research indicates that one of the largest security risks associated with mobile devices is actually end users themselves (Friedman & Hoffman, 2008; Educause, 2011). A study was conducted by Imgraben, Engelbrecht, and Choo (2014) in which two-hundred and fifty mobile device users from the University of South Australia were asked about their mobile device habits and practices. This survey indicates that users tend to be more lax with security measures on their mobile devices than they are with computers, stating that it is "not surprising that close to half of the survey participants reported not locking their devices (with password)" (p.1350) and yet "86% stored some form of personal information on the devices (password, login credentials and credit card information)" (p.1353). This same study focused on how participants connect to unknown Wi-Fi networks, stating that:

> About 48.4% of participants admitted leaving their Wi-Fi on at all times on their device. This increases the risk of them connecting to a malicious network and potentially exposing their data to an attacker (e.g. man-in-the-middle attack if users unwittingly connect to rogue wireless access point). (p.1354)

Approximately half of participants, if given a choice, would definitely or would consider connecting to an unknown Wi-Fi hotspot. The combination of private data being stored on these devices, risky end user behavior, and very poor end user security habits is a major reason why mobile device users introduce so much risk into the higher education environment.

A wide variety of devices.

Managing security risks for mobile devices also presents many challenges because of the wide variety of devices. Cheng (2007) stated that mobile devices differ in both hardware and software, and this variety can attribute to the difficulty in securing these devices. Devices may have differing computational capabilities, storage capacity, wireless interfaces, operating systems, and applications (Cheng, 2007). These variables work together to create a complex array of devices, which can further complicate a higher education institution's task of securing these devices. This diverse ecosystem of mobile devices can increase the cost of securing these devices (Cheng, 2007). Training staff, developing policies and procedures, and purchasing software solutions such as Mobile Device Management systems for a diverse pool of devices can be expensive. For an institution to undertake and maintain support of a variety of devices, it takes both an institutional commitment and institutional resources, which are sometimes both difficult to acquire.

Data loss.

One of the main risks surrounding mobile devices involves the loss of data via various methods. Verma (2011) stated that insecure data transfer should be particularly concerning for higher education institutions while the research of Mahesh and Hooter (2013) found that data theft is an important risk. They state that:

> users tend to download and carry far more data than they need on their devices due to a fear of not being able to access the data in the event of a loss of connectivity to the corporate database. This means that even the accidental loss of a MCD [mobile device] will result in significant data loss for the business. The

> damage from a deliberate, planned theft will be much worse. The loss can result in an adverse impact on business reputation, legal costs from losses of private customer data, and regulatory charges due to the failure to protect data secured by law such as healthcare related data. (p.5)

For higher education institutions that often deal with confidential data, FERPA and HIPAA regulations, this is no small risk.

Insecure data transfer.

An example of insecure data transfer is the capability of many mobile devices to provide a Short Message Service (SMS) and Multimedia Message Service (MMS), typically called text messaging and picture messaging. Erickson Press (2010) stated that mobile data traffic is now exceeding voice traffic in their live measurements. With this rise in popularity, people are sending more data via these methods, rather than using traditional e-mail or paper methods of transmitting data. These messaging protocols are a simple and cheap way to communicate but offer no security measures to protect data that are being sent or received (Enany, 2007). Enany (2007) studied the risks surrounding the SMS/MMS technology, as well as possible solutions to mitigate that risk. He proposed a model for what should be included in order to make these types of communications secure in the future. Enany (2007) stated that:

> In order to have an end to end secure communication channel, the following security services should be provided: *authentication, confidentiality, non-repudiation* and *integrity. Authentication* is to assure the recipient that the message comes from the source that it claims to be from. *Confidentiality* is to protect the data from unauthorized disclosure. *Non-repudiation* prevents both the

> sender and the receiver from denying/disowning a transmitted message. *Integrity* means that the message is received as sent with no modifications to the original message. (p.3)

While Enany's findings are valuable to the progression of security technologies, they also highlight another important problem. Many consider e-mail to be a secure means of communication today. However, using Enany's standards above, e-mail is not secure because it fails to pass the tests of authentication and confidentiality. E-mail can be "spoofed" to look as though it comes from one source, when it really comes from another. E-mail is not necessarily always confidential, depending on the method of transfer. If an e-mail is sent over an unencrypted network and in plain text with no encryption or added security, it can be viewed by unauthorized sources. As more and more institutions depend on e-mail, they have come to accept this risk as nominal and have chosen to continue to conduct business over e-mail. In the case of e-mail on a mobile device, the benefit of being able to use such a tool and the increase of productivity has outweighed the potential security risks. As the use of e-mail and SMS/MMS protocols on mobile devices continue to grow in usage, it is likely that institutions will have to make a choice. Do the benefits outweigh the risks? The freedom, flexibility, and popularity of doing so may outweigh the potential security risks of the medium, but policies and procedures may need to be introduced to the environment to ensure that confidential data are not transmitted via that mechanism.

The ability for mobile devices to connect to unsecured Internet connections also presents a risk that data could be transmitted insecurely. Yoon (2008) conducted research around the topic of network firewalls, studying the ability to effectively and efficiently

deploy firewall technology to protect network traffic at a particular location. While useful for those that are on-campus, this type of solution does not protect those that are doing business off-campus or those that are on-campus using unsecured Internet connections. Mobile devices have made faculty and staff increasingly mobile, and traditional methods of protecting a campus network do not go far enough to protect the data on those devices. With an increasing number of faculty and staff conducting business off of campus property, these security risks begin to take on a higher level of concern for higher education leaders.

Wang (2007) conducted a research study to examine security of communications in network environments. Most mobile devices have the capability of creating ad hoc mobile networks, sometimes called Wi-Fi hot spots, which are informal networks that can be created with no supervision or permission anywhere there is cellular service. People share a network connection through this ad hoc network, often with little to no security around it. The flexibility and mobility of the network is a driving reason for people to use these types of networks. However, because these networks are not secured, policed, or standardized, confidential data may be at risk for those who utilize them.

Malware and viruses.

Another risk associated with mobile devices is the risk of malware or viruses which could infect the phone, but more importantly, steal private or confidential data (Verma, 2011; Mahesh & Hooter, 2013). Ongtang (2010) conducted a research study to examine mobile device security, determine the current limitations, and propose a model to secure mobile phones in a constantly changing ecosystem. The researcher proposed placing a piece of software onto mobile devices which certifies applications as safe and

helps protect the phone from applications that may present a threat to the mobile device. Again, these types of software which impose policies on mobile phone users, may help prevent security issues but also potentially prevent the installation of certain applications that faculty and staff may desire to have placed on their mobile device. Institutions must weigh the options and determine if enforcing such policies on mobile devices inhibits the faculty or staff person from being able to conduct their work. If so, it may not be in the institution's best interest to employ these policies, as academic freedom and employee productivity may be hindered by doing so.

How to Manage the Risk of Mobile Device Security

Once institutions have learned which mobile device security risks they should be most concerned with, the literature demonstrated that there are several areas in which leaders should pay particular attention in order to successfully manage the risk of potential security incidents. As described above, software and technology solutions such as a Mobile Device Management system with security rules preventing misuse can often be used to prevent security breaches (Wang, 2007; Verma, 2011; Yoon, 2008; French, Guo, & Shim, 2014). Another area that should be examined by leaders is institutional policy and staffing to write and support those policies (Mahesh and Hooter, 2013). According to the EDUCAUSE Core Data Service:

> Institutions with a chief information security officer or other full-time staff member devoted to information security are more likely to have implemented security practices and related technologies such as scanning and patching institutional systems, encrypting data, and mobile device management. (p. 11)

One of the most widely espoused areas that leaders should focus on is end user education. Imgraben, Engelbrecht, and Choo (2014) found that "many end users are generally unaware of the risks that they may expose themselves to every day and that these users do not receive sufficient education regarding their smart devices' usage and security" (p. 1357). The final area institutions should examine is their resource allocation model for information technology security. Literature shows that these areas are where higher education leadership should be looking in order to prepare their institutions in order to prevent potential mobile device data breaches and security issues.

Software and technology solutions.

Software and technology solutions is often the first area of which technology security personnel think when discussing what can be done to secure mobile devices. Mobile Device Management (MDM) systems, once touted as the way to control mobile devices and force adherence to more secure practices, are still an important part of the mobile device security solution (French, Guo, & Shim, 2014). Friedman and Hoffman (2008) suggest that firewalls, anti-virus, anti-spyware, intrusion prevention detection systems, malware protection systems, encryption, backup and recovery software, device controls and policies, and enforcing passwords are all possible technology solutions to mitigating risk for these devices. There is a vast array of options to choose from, and institutions must pay careful attention to which systems will provide the most value in their environments without inhibiting the academic mission. In addition, technical systems which enable institutions to use these tools are only part of the solution. Recognizing the tidal wave of mobile devices entering our environment, it is important

that higher education institutions create a comprehensive solution which does not depend completely on MDMs or technology solutions.

Institutional policy.

Institutional policy is another solution for administrators to critically examine (Mahesh & Hooter, 2013). Because mobile devices are new comparatively to other types of technology, many current institutional policies and procedures do not address mobile devices specifically. A study focused on a panel of professors at several U.S. universities and found that there are large gaps in current policy, putting the institution at risk (French, Guo, & Shim, 2014). In a 2014 doctoral research study conducted by Fuller, he examined the existing policies at the Winnetka Public Schools District 36 and found that the school's current policies did not address devices, recommending that current policy be reviewed and new policy suggested in tandem. Joel (2010) states that:

> Technology is complex, difficult to understand and describe, and continues to change rapidly. It is, therefore, a daunting task to pose to lawyers, policy makers, and the rulemaking process to capture the essence of technology's implications—in all its richness—and in a way that will enable its effective use (p.1763)

Because policies either do not exist or old policies do not exactly apply to these new devices, many end users choose to manage their devices in a variety of ways, some of which are not secure. For example, Clarke and Furnell (2005) conducted a survey of 297 current or previous cellphone subscribers via an online questionnaire over a period of two years. The researchers found that 34 percent did not use any PIN security at all. The 2014 study conducted by Imgraben, Engelbrecht, and Choo stated that approximately half of participants did not use any type of PIN or locking security, suggesting that users have

not become more cautious in the past nine years. A simple policy which mandates a password or PIN be used on a cellphone, smartphone, tablet, or other mobile device could help ensure that users are protected in this area. Friedman and Hoffman (2008) state that "Security policies must be defined, documented and published to end users before they can be enforced" (p.18).

However, research has also demonstrated that many techniques that universities may mandate that faculty and staff use to protect their mobile devices may actually inhibit usage of the devices and make them less easy to use. French, Guo, and Shim (2014) state that:

> Another troublesome fact is the imbalance between work productivity and policy. An overzealous policy is unfavorable for employees' morale, but a poor policy may lead to tardiness and distractions from work. (p.194)

For example, requiring faculty and staff to use a PIN on their mobile device can actually inhibit usage of the device, making it less convenient to use, while not having a PIN means that anyone could pick up the device and potentially access confidential or private data. Researchers Botha, Furnell, & Clarke (2009) studied the similarities of protecting a Windows XP computer and a Windows mobile phone using similar security techniques. The researchers found that, although the same elements of security are available, implementing them on a mobile device causes a significantly higher impediment to use than when implementing them on a desktop computer. In implementing security measures that may affect the usage of the device, it is critical that higher education institutions weigh their options. Certain types of security, such as forcing faculty and staff to set a PIN, may create minimal problems for usage and are possibly quite

reasonable for an institution to require and enforce. However, other types of security, such as restricting application usage or mandating a specific brand of device, may not be as reasonable and may cause undue hardship for faculty and staff who want the freedom to choose their own devices to use.

End user education.

Human behavior is frequently blamed for the majority of security breaches. Researchers Brechbuhl, Bruce, Dynes, and Johnson (2010) stated that "if you are on the network, you are available to everyone else on the network. A key consequence is that security is not the concern of someone else; of necessity it is the concern of everyone" (p. 84). According to a report by Educause Center for Applied Research (ECAR), information security has traditionally been viewed as an IT problem, but in today's modern University, security issues can no longer be pushed on to the information technology department to handle (Boes, Cramer, Dean, Hanson, & McKenna, 2006). This becomes especially true when faculty and staff utilize their mobile devices off-campus on systems over which the IT department has no control. Therefore, security issues must be addressed by all of the users, not just the administration.

Increased training for employees is often touted as a core solution for preventing breaches in the future (Turner, 2011; McElroy & Weakland, 2013). Gartner (2010) recommends that users must be educated to the risks, and the institution must create policies to guide their behavior in safe ways. In a study conducted by CDW-G (2009) about federal government cyber security, user education was cited as the number one defense against security breaches. Baker and Wallace (2007) stated that "Technical approaches alone can't solve security problems for the simple reason that information

security isn't merely a technical problem" (p.37). Going one step further, Imgraben, Engelbrecht, and Choo (2014) suggests that:

> that any educational materials developed for smart mobile device users need to be tailored specifically to the user group (e.g. Generation X, Generation Y, and baby boomers; and end users from diverse cultural and linguistic backgrounds) and end users with varying technical backgrounds. (p.1358)

This study surmises that a poorly implemented user education program will not aid in reaching the goals of improved security, so it is critical that higher education institutions study current security-focused educational initiatives and develop their model on proven user education techniques. In a study conducted by Educause to examine higher education institutions' current training models, it was found that the most popular forms of training are digital ones, with 57 percent of survey respondents utilizing online training, 54 percent utilizing website educational materials, and 51 percent using e-mail (McElroy & Weakland, 2013, p.2). Sixty-two percent of those surveyed measured their success by the number and type of security incidents, while 45 percent measured their success by employee feedback. Of those surveyed, 73 percent said that their institution does not measure the return on investment of security training and awareness. The study concludes that "institutions should carefully consider how a proposed effort or technology can produce quantifiable and objective metrics" (McElroy & Weakland, 2013, p.8). Without these metrics, institutions will have no idea if their methods are working, if their end user population is getting the message, and if the institution is getting a return on their investment with regard to security training.

One of the problems for administrators is that, in each of the scenarios described above where an end user experienced a security breach, the person impacted may or may not even have known to contact the University IT security officials to let them know of a data breach. Data breaches often can go undetected for long periods of time, making it even more difficult to attempt to clean up the mess. Security can be a hidden problem. Because security is not something one can see or feel, problems with the security of systems are often invisible to those at the institution until a security breach occurs. User education should focus not only on prevention, but also on how to detect a breach and what to do if a security issue is suspected (McElroy & Weakland, 2013).

Resources for security.

Research indicated resource allocation for information technology security can also be an issue (Boes, Cramer, Dean, Hanson, & McKenna, 2006). Because mobile devices have not been around as long as other types of technology, many higher education institutions do not have resources specifically allocated to the support of these devices. Resources needed may include funding for hardware, software, and staff, but may also include time of current staff to support these devices or discuss and write policies and procedures for how to address the handling of these devices. This is not a one-time investment. As the industry and security threats continue to evolve, it is critical that institutional policy be able to be adapted to address the changing landscape. French, Guo, & Shim (2014) state that:

> The rapidly changing IT landscape require solutions that deliver visibility and insight that assist organizations to make informed decisions, create reliable action plans, and monitor ongoing progress. (p.196)

This means that resources must remain focused on this area well into the future. Institutions must determine what resources they are going to allocate towards data security on an ongoing basis in order to be successful in developing a plan for preventing mobile device security issues.

Conclusion

The purpose of this research study is to further investigate each of these topics and learn about how institutions are handling these security issues today. At each institution being studied, the researcher explored policies, methods of user education, and the types of funding and staffing resources which are being currently allocated towards mobile device security. By creating a picture of what institutions are doing today and how they plan to address mobile device security in the future, this research study sought to provide information for higher education leaders as to how they can address mobile device security at their own institutions.

CHAPTER 3 - METHODOLOGY

Research Design

This study was a qualitative study in the form of case studies about how institutions handle mobile device security today and what they plan to do in the future. Four institutions were chosen as the setting in which to examine mobile device security, and three to four individuals were interviewed at each institution. The reason for using this design was to fully delve into each institution's policies, procedures, and practices around mobile devices. Conducting in-depth interviews with multiple sources allowed the researcher to fully explore the ramifications of mobile device security at each institution. By utilizing qualitative methods, the researcher was able to more fully describe the measures institutions are taking to secure mobile devices. This will assist in creating a picture of what institutional leaders need to know about mobile devices and how to best address securing them for the future.

The study best fit the design of a multicase study which involved "collecting and analyzing data from several cases" (Merriam, 2009, p.49). This research was based on the framework outlined by Merriam (2009). Qualitative data were collected by conducting interviews at the four selected institutions, and the data were compiled into a case study of each individual institution. This allowed the researcher to create a picture of the overall mobile device security environment at that particular institution. Each institution's individual characteristics were studied, although the actual institution names will remain confidential. The processes that each institution utilizes to secure mobile devices are outlined, as well as any successes or failures the institution had experienced regarding mobile device security. Following the creation of the four case studies, these

institutions were examined together to create a model of how some institutions are addressing mobile device security. Merriam (2009) stated that "the inclusion of multiple cases is, in fact, a common strategy for enhancing the external validity or generalizability of your findings" (p. 50). The data from all four case studies were utilized to create a list of best practices across institutions, the goal of which is to assist other institutions in knowing where to start when preparing their own institutions to address the extremely large task of improving the security of their institution's mobile device landscape.

The data were collected in the form of semi-structured interviews with key IT staff, administrators, and faculty at these institutions. The initial interviews were between 30 and 60 minutes in length. They were conducted over the phone and most were recorded if the interviewee gave consent. Each participant signed an informed consent form letting them know of the purpose of the study, the risks, and that they could stop the interview at any time. This form also asked if they were willing to be audio recorded. Most participants agreed to be recorded.

The recordings were transcribed by a third-party unaffiliated with the research. The company doing the transcription signed a confidentiality agreement. The researcher took detailed notes during the interview of key concepts that arose. This greatly assisted in tracking common themes across interviews. Following the initial interview, a few follow-up interviews with some of the participants were conducted. These were approximately 30 minutes in length and were conducted to answer any remaining questions.

After transcription, the data were reviewed, coded, and analyzed. The researcher organized the data in two ways. First, the researcher examined each institution

individually, looking at the institutional characteristics pertaining to the IT environment. Second, the researcher examined all institutions together to look for similarities and differences across all of the organizations.

In addition to the interviews, the researcher explored institutional data, including policies, procedures, and regulations. This included policies for the institutions as well as policies for the states in the Midwestern United States if the institutions fall under the jurisdiction of the state. Federal regulations such as FERPA, HIPAA, and PCI were examined. Resources and materials made available to the constituents of the institutions regarding mobile device security were also examined. This included online and printed materials, trainings, and technology standards if the researcher was able to find them publicly available. It was critical to conduct a review of the types of devices and access provided to students, faculty, and staff at each institution in order to gather a full picture of the risks and how they are being managed.

Interview challenges.

Obtaining interview participants was a major challenge of this research study. The first hurdle involved obtaining permission from the institutions that were chosen to be studied. The second hurdle involved finding individuals at each of the institutions who were willing to be interviewed.

When the researcher first proposed this study and was approved, it was designed to be a national study. The IRB asked for the four institutions being studied to submit a written letter or e-mail indicating consent. When the researcher approached the originally chosen institutions, one institution readily agreed and sent the appropriate e-mail. The other three institutions each stated that they had no issues with the research being

conducted on their campus since it did not involve any kind of confidential or sensitive data, but that they had no authority to officially approve the study to occur on campus property. Because they were unable to write letters on behalf of the institution approving the study, the researcher contacted many different departments at each institution seeking this approval. Each area contacted indicated that they did not have the authority to write letters agreeing to participation, and the researcher was unable to obtain written permission, which was necessary for the IRB approval to go through. Eventually, the researcher placed the study on hold for two years.

After the researcher resumed the study, the researcher updated the literature review and selected new institutions for the study based on a regional study. The researcher focused on the Midwestern United States. The researcher determined that it may be easier to obtain permission and the appropriate connections at institutions in closer proximity. This would enable the researcher to travel to conduct the interviews in person, which the researcher also thought would assist in obtaining consent to conduct the research.

Once the new institutions were approached, one institution agreed readily and provided the necessary documentation. The next institution had a form that the researcher needed to fill out. Once this was done, they approved and provided the correct paperwork. The third institution determined that they did not need to review the research at all as long as the interviews were conducted off-campus. The institution provided documentation indicating that this was the case. The IRB approved the study to begin with these three institutions while the researcher worked to obtain approval from the final institution.

The researcher began interviews at the three institutions. In all cases, schedules for the selected individuals were extremely challenging to coordinate. Because the interview subjects had very pressing schedules, the researcher had to be available at their discretion. The first subject only had one hour the very next day, and the researcher was unable to drive to get there in time, so that interview was conducted over the phone. Over the course of the next two months, the rest of the interviews were scheduled and conducted. Because the people being interviewed had vast scheduling differences, all interviews were conducted over the phone. Interviews ranged from 30 minutes to 60 minutes in length. Due to the difficulty in obtaining agreement to be interviewed, the researcher was sometimes only able to get 30 minutes of the interview subject's time. Despite the shortened length of the interviews, the researcher was always able to ask all of the research questions without rushing the interview participant.

During this time, the researcher was still working to obtain permission from the final institution. Meanwhile, one of the individuals previously interviewed left that institution and took a new job working at the final institution. The researcher learned that the IT community is a small environment, and there is often overlap as IT leaders move between institutions in the region. At this time, the researcher decided that it was unwise to study this institution at this point, because she would be re-interviewing an individual she had already interviewed. A new final institution was chosen. The institution stated that they did not need to approve the study and that interview subjects were free to participate in the study if they chose. The IRB approved the addition of the final study.

The second major hurdle in obtaining interview participants was getting participants to agree to be interviewed at all. As the researcher began reaching out to

individuals to request their participation in interviews, a few agreed readily. However, the vast majority were unwilling to be interviewed. As the researcher approached individuals requesting interviews, the researcher received over thirty responses declining to be interviewed.

When citing why they were declining to be interviewed, the researcher compiled two main reasons. The first reason potential participants declined to be interviewed was because they felt that they did not know enough about that subject. Many interview subjects stated that this was not their area of expertise; they did not know what their institution was doing about this topic; or that there was someone else who knew more that the researcher should be interviewing instead. The overall theme was that they did not feel that they could contribute enough information to be of use because the topic was not something they knew that much about. This could speak to the research finding that there is not enough communication and end user education about mobile device security today.

The second reason that participants declined to be interviewed was because they were concerned that the information they shared could potentially expose their institution to harm if a potential attacker was to learn too much about their security environment. These individuals stated that they did not want to accidentally disclose any confidential information and that they were uncomfortable conducting any interview that might highlight their vulnerabilities to a potential attacker.

Despite these challenges, the researcher was still able to obtain sufficient interview subjects to conduct the study.

Study population and sampling plan.

The researcher compiled four case studies for the qualitative portion of this research study. These case studies feature four-year institutions only.

Table 1

Sample Population

	Numbers of Students	Numbers of Employees	Type of Degrees Granted	Public or Private?
Institution A	Over 10,000	Over 2,000	Undergraduate and graduate	Public
Institution B	Over 30,000	Over 15,000	Undergraduate and graduate	Public
Institution C	Over 30,000	Over 15,000	Undergraduate and graduate	Public
Institution D	Under 5,000	Under 400	Undergraduate only	Private

Samples were chosen by using the purposeful sampling technique. Institutions were selected by the researcher based on their reputation as a leader in the field of technology within the Midwestern United States, using a technique called extreme case sampling (Creswell, 2008). These institutions were particularly enlightening as they may be leaders in the area of mobile device security. Institutions were approached by the researcher through phone and asked to participate in the research study. Typically, the Institutional Review Board (IRB) was the first point of contact, after which the IT department was contacted.

Once the institutions were selected, the researcher again utilized the purposeful sampling technique and the cooperation of the institution to choose three to four individuals to interview at each site. Interview participants were chosen based on their role and expertise within the field of technology, security and/or institutional policy, or as

a faculty expert using a technique called reputational-case sampling (Creswell, 2008). Once participation was agreed upon with the institution, the researcher utilized basic web searches of each institution's web sites to obtain the phone numbers of several faculty, staff, and administrators who have particular expertise or experience with mobile device security at that particular higher education institution. The participants were approached by the researcher first through phone correspondence and e-mail. The potential interview participants were given basic information about the study and asked to participate in the research study. They were told there would be no negative ramifications to themselves or their institution if they declined participation.

Description of research participants.

The researcher asked each interview subject to briefly describe their background and role at their institution. Institutions are further described in Chapter 4. Supplemental background information was collected in follow-up conversations with the interview participants and from the LinkedIn profiles of the interview participants. Pseudonyms were used to protect the identity of the research participants.

Institution A

Victor Samuels – Chief Information Officer: Samuels is responsible for providing strategic direction to the University on technology for all academic and business units. He provides executive leadership in technology solutions, services, and infrastructure in order to promote the University's strategic plan. Samuels stated that:

> My role is to ensure that technology is used to advance student and faculty success, ensure the service and process is pertinent, and provide superlative

> access to data. I'd say that's pretty much the key role of a CIO at any higher education institution. (Victor Samuels, Interview, 2015, 01:56)

Samuels has been a CIO for over fourteen years, four of those years specifically at this University. Prior to becoming a CIO, Samuels spent four years as a Technology Director in another large institution within the Midwest region of the United States.

Luke Jackson – Assistant Chief Information Officer / Director of Technology Services: Jackson is on the management team and assists the CIO with planning around the University's technology strategic plan. In addition, Jackson stated that his team is responsible for:

> The network servers, telecommunication and communication systems, and then we work with integrating services too, because all software needs to know about other software, and the daily integration that happens between those. (Luke Jackson, Interview, 2015, 00:09)

Jackson has worked in this role for the past fifteen years. Prior to coming to this institution, Jackson spent two years as a systems engineer in the private sector.

Kurt Adamson – Chief Information Security Officer: Adamson is responsible for providing information security leadership through the continued development and implantation of an information security program at this institution. This is a brand new position, and Adamson has been in this role for the past few months. Adamson describes his role as allowing students, faculty, and staff "to learn, teach and work in a safe, secure environment" (Kurt Adamson, Interview, 2015, 01:29). Prior to this, Adamson worked in the IT Systems area of this institution for over six years. Before to coming to this

University, Adamson worked in the private sector for over eleven years in various IT roles including Network Administrator and Systems Administrator.

Everett Douglas – Professor: Douglas is a faculty member at this institution and specializes in security. For the past ten years, Douglas has been teaching, researching and writing, and creating and designing technology security courses. Douglas also consults on technology security for businesses and higher educational institutions. Douglas stated:

> In addition to teaching security, and again, spending the past three years creating a brand new fully aligned master's degree program leveraging courses from the college of business, I've also spent the past ten years doing security consulting. (Everett Douglas, Interview, 2015, 1/04:16)

Douglas has worked as a faculty member at this institution for over fifteen years.

Institution B

Duncan Brooks – Senior Manager of Technology Support: Brooks is responsible for managing the University's workstation support groups within the central IT department. His team supports the workstations in the department as well as customer departments across the University. They also provide a fee-based support service for personally owned computers for staff and students of the University. Brooks stated that:

> We run a matrix-managed IT organization. So we have folks like myself who manage people and functions. And then we have service structures who manage services. And they ask the functions people to deliver those services. So I manage our service desk staff and the function of the service desk. And then other services, like our e-mail service, would say, "Hey, I need people to help support

> e-mail." And I would allocate effort from my team to do that. (Duncan Brooks, Interview, 2015, 00:17)

Brooks has been in this role for over three years and at this institution in various IT roles for over fourteen years. Prior to coming to this University, Brooks worked in the private sector as a computer engineer for one year.

Matthew Hudson – Chief Information Security Officer: Hudson is responsible for providing security, vision, planning, and leadership for the University's information security program. He provides short-term and long-term planning, provides information security expertise to all aspects of the University, and ensures compliance with mandates such as HIPAA and PCI. As the leader of the security department, Hudson acts as the liaison with other business entities within the institution and serves on leadership committees across the organization (Matthew Hudson, Interview, 2015). Hudson has been in his role as CISO for nearly four years. Hudson has worked in the field of information security for over seventeen years. Prior to coming to this institution, Hudson worked in the private sector for six years as a director of security. Before that, he was employed in a variety of leadership roles in the area of finance and technology in the private sector.

Kyle Lawrence – Chief Information Officer of a large college within the University: Lawrence was previously responsible for all technology support and infrastructure within the college, but his role has recently shifted. In the past year, basic support of computers has moved to the central IT department. Lawrence stated:

> We got out of the business of doing help desk and desktop support. That shifted to central IT last year. We did that for a couple of reasons: one, budget-wise, the

> college had a pretty tight couple of years there; and, two, because that shift of moving away from the people that fix the computers allows us to get a different relationship with the faculty, students, and staff. (Kyle Lawrence, Interview, 2015, 00:08)

Lawrence is responsible for working directly with instructors and researchers within his college to ensure that technology support their mission of teaching and learning. Lawrence has been in the CIO role for the past three years, and prior to that, spent seven years working at the University in various other IT roles.

Institution C

Michael Gregory – Chief Information Security Officer: Gregory is responsible for all IT security on all campuses within the entire state system, including over 20 individual campuses. This includes some four-year institutions and some two-year institutions. Gregory acts as the security liaison across departments, including outreach with faculty and staff, as well as with other business executives. He is responsible for all IT security staff and guiding them on implementing security functions. He is also responsible for creating a security strategic plan for the institution and overseeing security training opportunities. Gregory has been in this role for less than one year. Prior to that, Gregory spent thirteen years as a technology security consultant. Before moving to that career, Gregory spent nine years managing information security professionals for a branch of the government and twenty years working in a division of the U.S. Armed Forces.

Kevin Johnson – Assistant Director / Help Desk Manager: Johnson is responsible for all aspects of technology support. Johnson's area provides support across the entire

campus to anyone who is affiliated with the University for any service that is provided by the central IT group. Johnson stated:

> That would be student information systems, learning management systems, identity management systems or access management systems, I guess, you would call them. That's a fancy way of saying we do a lot of password resets [laughter]. We provide support across any tool that any person who's affiliated with the University chooses to use to further their contribution to the mission of the University. We are one of several help desks on campus. I don't have a count of the number of help desks we have on campus, but it's probably, if I were to venture a guess we probably have ten or so across campus who provide support at varying levels. But we are, by far, the largest. (Kevin Johnson, Interview, 2015, 00:08)

Johnson has been in this role at this University for three and a half years. Prior to that, he spent nine years working in technology support management at another University outside of the Midwest. Before taking that position, Kevin spent eleven years working in the private sector at various companies, and his roles were focused on technology support at varying levels.

Dylan Weston – Security Consultant at a department within the University system: Weston's primary role is to assist the department with any security initiatives. Because the institution is extremely large and has a decentralized IT department, some departments hire their own IT personnel. Weston was hired to bring "all the machines up to a standard level of security" and his role has expanded since then (Dylan Weston, Interview, 2015, 00:08). Weston stated, "We do our best to try and get them connected,

and try to help them, essentially, do their job" (Dylan Weston, Interview, 2015, 05:22). Weston has been in this role for a year and a half, and prior to that, he worked for nearly four years as a systems administrator in another department on campus.

Alex Bennett – Assistant Director of Campus Network Services: Bennett is responsible for all network functions for this University, including the wired and wireless infrastructure. He stated that his team has:

> The responsibility of the overall design architecture of the campus wired and wireless network, and my team also provides third tier support as we work through issues that come up with the network that are affecting service or performance or features that we want to implement. (Alex Bennett, Interview, 2015, 00:06)

Bennett has been in this role for two and a half years, though he has worked at this institution in various IT roles for the past seven years. Prior to coming to this institution, Bennett spent over 14 years working in a variety of technology and network engineering roles within the private sector.

Institution D

Arthur Williams – Chief Information Security Officer: Williams has responsibility for the entire technology security environment at this college. Williams was recently appointed to this newly created position and had only been in the position for a few weeks at the time of the interview. Williams stated that:

> As far as security was concerned, it was pretty much handled by various people depending on their role. The infrastructure person handled infrastructure security, the apps team had their own kind of security. But I think they got to a point where

> they just said, "You know, we've got to consolidate the security all in one and bring in policies and procedures." I think a lot of pressure was put on them by BYOD. They didn't have a Bring Your Own Device policy in place. When I interviewed for it, they said this position probably should have been filled 20 years ago. So that's kind of, in a nutshell, why they hired me. (Arthur Williams, Interview, 2015, 00:06)

Prior to accepting this position, Williams was an IT director for over nine years at a large agency employing over 1,000 individuals. Prior to that, he was network administrator at that same agency for approximately eight years.

Grace Jones – Professor: Jones has been a professor of Computer Science for the past nine years and has worked at this institution for her entire career. She had recently left the institution during the time of the interview to begin a new position at another college. Her expertise is in a wide range of areas, including computers, networking, mobile device usage, social media, and software development.

Cody Grayson – Senior Instructional Technologist: In this role, Grayson works with faculty and staff to utilize various types of technology for instruction. He trains faculty and staff in large groups and one-on-one settings, assisting them in using technology to meet their educational goals. Grayson has been in this role at this college for eleven years and describes his role as "essentially, I help faculty apply technology in their courses. (Cody Grayson, Interview, 2015, 00:06).

Interview procedures.

The researcher utilized the following steps to collect interview information:

1. Contacted (through phone and e-mail) selected institutions to determine willingness to participate in research study (began March 1, 2015).
    a. Disclosed procedures with clear expectations outlined for the participants about time commitments and nature of the interviews.
    b. If institution agreed to participate, institution representative will sign Informed Consent Form.
2. Contacted (through phone and e-mail) selected individuals to determine willingness to participate in research study (began April 1, 2015).
    a. Disclosed procedures to all participants with clear expectations outlined for the participants about time commitments and nature of the interviews.
    b. For participants who have accepted, e-mail them an Informed Consent Form outlining expectations and asking for their permission to participate in the study and audio-record the interviews.
3. Conducted interviews over the phone (completed by July 2015).
    a. Interviews were audio-recorded, if consent was given, and the researcher took thorough notes.
4. Coded and analyzed interview data (completed by July 2015).
    a. Ensured anonymity of the participants by assigning pseudonyms to individuals and organizations.
5. Conducted follow-up interviews as needed (completed by July 2015).
    a. Interviews were audio-recorded, if consent was given, and the researcher took thorough notes.

6. Coded and analyzed additional data along with original data (completed by July 2015).
7. Completed final dissertation draft (completed by August 1, 2015).

Interview protocol.

The interview protocol developed included open-ended questions to provide ample opportunities for interviewees to elaborate. Interview questions included multiple probes into the central question and sub-research questions. The interview questions are provided in Appendix F. They were designed to elicit how the individual and the institution address the topic of mobile device security. Often information provided by the interviewees led to follow-up questions into the specifics of their organization's environment and their own specific security expertise.

Interviews were conducted over the phone and audio-recorded. Interview subjects were informed of the audio-recording at the beginning of the conversation, and asked again if they consent to be recorded. After gaining consent, the interview participants were informed of the basic purpose of the study. At the beginning of each interview, the researcher made sure that the interview subject had read through and agreed to the informed consent form. Following these explanations, the interview questions were asked while allowing interview subjects time to elaborate on each question. Probing sub-questions were asked as various topics arose. One follow-up interviews was conducted to further explore the breadth of two of the interview subjects' expertise in the area of mobile device security.

Data analysis plan.

The data analysis plan was developed utilizing techniques outlined by Creswell (2008) and Merriam (2009). First, the data were organized and a matrix of all sources was compiled to ensure accuracy of records. The audio recordings of the interviews were transcribed verbatim by a third-party who was uninvolved with the research in order to ensure accuracy of records and eliminate bias. The researcher first scanned the data for accuracy. Next, it was imported into nVivo and prepared for analysis by using descriptive coding. During this process, the researcher read each sentence and assigned topics to each sentence. As similar topics emerged, these became the codes used by the researcher. Finally, the researcher explored the data and looked for various themes from within the data. The process for examining the data was iterative, and it continued to cycle between data collection and analysis. Interviews were conducted, uploaded into the system, coded, and then additional interviews were conducted in two cases where the researcher wanted further explanation.

All printed records and audio-tapes were maintained in a locked file cabinet, and they will be disposed of through a secure documents disposal company. All electronic records were stored on an encrypted hard drive which will also be stored in a locked filing cabinet before being securely erased. Only the principal investigator has the key to unlock these records. Individuals and institutions who participated in interviews were not identified by name on records kept. They were assigned pseudonyms at the beginning of the research study, and this pseudonym was used on all records kept. Records are intended to be kept for a period of three years from the beginning of the research study.

Following the coding, the researcher scanned the codes and linked similar codes together to create larger themes. The researcher used the same coding process for each interview in order to examine each institution individually and then connect the codes that spanned across multiple institutions. This allowed the researcher to find themes that applied to more than one institution. Next, the researcher made comparisons between the themes from the literature and the themes from the interview data. In Chapter 4, each institution is examined on its own; but, furthermore, all four institutions are also examined for themes common to the whole group.

Verification procedures.

Merriam (2009) stated that "though qualitative researchers can never capture an objective 'truth' or 'reality,' there are a number of strategies that you as a qualitative researcher can use to increase the 'credibility' of your findings" (p. 215). Merriam outlines several techniques to enhance credibility, and the researcher chose three of these methods which are well-suited for this particular research study. The researcher utilized the following three strategies for verification purposes during the research project:

- Member checking (Merriam, 2009, p. 217): Because the interview subjects are the experts on this topic, bringing the final themes and paper back to a few of them for their review was a critical piece of the verification process. The researcher selected two interview subjects with which to share a draft of the final research paper. This enabled these interview subjects to review the information provided and the final results of the study to determine if they feel their information was presented accurately and correctly by the researcher. In

addition, it allowed these two interview subjects, who are experts in the field of mobile device security, to provide feedback for the improvement of the study.

- Researcher reflexivity (Merriam, 2009, p. 219): The researcher is employed in the field of information technology at a higher education institution. As such, the researcher has personal views and potential bias that may come through in the research study. The researcher wrote a section in the final chapter which outlines these personal biases. This "allows the reader to better understand how the individual researcher might have arrived at the particular interpretation of the data" (Merriam, 2009, p.219).
- Peer review (Merriam, 2009, p. 220): The researcher asked peers and colleagues to review the themes and the final paper. These experts in the field of information technology were able to assist in reviewing the themes and determining if they were correct according to their own knowledge and if they were correctly represented by the researcher's paper. In addition, two faculty members were selected to review the findings and provide feedback. Having experts review research can assist in lending credibility to the research study and can help readers feel more comfortable with the research.

Ethical Considerations

Merriam (2009) stated that "although policies, guidelines, and codes of ethics have been developed by the federal government, institutions, and professional associations, actual ethical practice comes down to the individual researcher's own values and ethics" (p.230). The researcher has made an effort to disclose every step of the research process to eliminate questions about methods and assist in allowing others to see

the entire process that was followed. The researcher has thoroughly discussed the research and findings with interview subjects during the qualitative study to ensure that their participation in the study is handled ethically. Informed consent forms were signed to ensure that interview subjects were made fully aware of any risks associated with the study.

Role of the Researcher

In a qualitative study, it is critical that the researcher gather and analyze data, which then produces meaningful information. The goal of the researcher is to refrain from imparting their own personal bias on the information. Though it can be difficult to remove all bias, the researcher has attempted to document any bias prior to beginning the research.

The researcher is disclosing that working in the field of technology may increase bias toward this specific topic, as the researcher has formulated many opinions through experiences at work. However, every effort was made to separate those biases from this research and let the interview subjects speak for themselves. The researcher documented perceptions in a journal-like fashion after conducting the literature review prior to beginning the interviews in order to ensure full disclosure. The purpose of documenting the researcher's perceptions was not to determine if the researcher was right or wrong, but simply to document the researcher's perceptions in order to ensure that they did not influence the final results of the study.

The researcher's assumption after conducting the literature review was that the policies and procedures adopted by institutions in the Midwest are likely focused on the devices themselves, lagging behind focusing on the data assets themselves as the research

is pointing towards as the future of mobile security. Another assumption the researcher had was that the institutions, if they have mobile device policies, probably had separate mobile device policies for students versus employees.

The research showed that if institutions have a Chief Information Security Officer (CISO), they likely have more concrete policies than institutions without a CISO. However, the researcher expected the appointment of an actual CISO to be rare, as often the research stated that resources and funding around security and security-related positions was limited. Security is often touted as an unseen risk and therefore too easy for institutions to ignore it. Because of this, the researcher expected that all the institutions would state that they do not have enough resources dedicated towards security.

The researcher's assumption was also that there would be huge concerns about the BYOD movement and the lack of knowledge of what people are accessing and from where. The researcher expected there to be little data about what people are doing on their mobile devices, how they access information, and how they dispose of their devices. The researcher also expected that there would be very little in the way of training for students and slightly more resources to train faculty and staff on security.

Creswell (2007) states that documentation of our biases is important, as evidenced by his statement, "In the entire qualitative research process, the researchers keep a focus on learning the meaning that the participants hold about the problem or issue, not the meaning that the researchers bring to the research or writers from the literature" (p. 39). By documenting assumptions, the researcher hoped to present plausible findings based on the collected data and maintain transparency on any biases.

CHAPTER 4 – RESEARCH DATA

Introduction

This chapter informs the reader on the research findings of these interviews and examinations. This included four individual case studies and a cross-case analysis to bring together those interviews in a cohesive manner. Pseudonyms were used for each interview subject to protect their identity and the identity of their institution.

Case Study #1 – Institution A

Introduction.

Institution A is a medium-sized undergraduate and graduate degree-granting institution. Located in the central region of the United States, this institution serves over 10,000 students and over 2,000 faculty and staff. This institution is a part of a larger system of institutions who are all separate but collaborate on certain high-level initiatives including security-related issues. Instruction happens via a variety of methods including face-to-face, online, and distance learning.

Interview subjects included Victor Samuels, Luke Jackson, and Kurt Adamson, all from the central IT department, as well as Everett Douglas, a faculty member who specializes in security.

Environment and staffing.

The following questions were asked by the researcher to assist in creating a picture of the environment at this institution:

- Please describe the role you take in working with mobile devices and/or security at your institution.

- What do you think the perception is of the security of mobile devices by the faculty and staff?
- What do you think your institution does well regarding the security of mobile devices?

The IT staff are primarily centralized in organizational structure at this institution, but some of the physical locations of staff are distributed. Adamson stated:

> We have our central service desk. And we also have technology directors embedded into a few of our colleges. So they're there as a resource, not necessarily for service desk, but they're there as a resource. (Kurt Adamson, Interview, 2015, 07:42)

Out of a workforce of approximately sixty IT staff members, there are two IT staff specifically dedicated to security in various aspects (University web site). These two IT security staff members are housed within central IT and function as a part of that department. Support of security is not limited to just those two individuals, however. Other parts of IT, such as help desk areas, handle some security issues as they are reported from faculty, staff, and students.

This institution had a previous security manager position within their IT department and has transitioned that role to a higher level security position this past year. Adamson stated that “this is the first CISO position” for the institution (Kurt Adamson, Interview, 2015, 00:51). According to Adamson, the driver was “the increase in need for security” and “ensuring that security is made a priority for the campus” (Kurt Adamson, Interview, 2015, 01:13). Adamson sees the role of the CISO as a business enabler who

allows students, faculty, and staff to operate in a safe environment. Adamson explains that:

> The way I've written the position for information security is to enable students, faculty and staff of [Institution A] to learn, teach, and work in a safe, secure environment. I'm really positioning things to be a business enabler. Some people look at security and take security as, "You must do this, you must do that," and "You cannot do this, you cannot do that." I don't want to be that. I want to be somebody who enables the business to function in a secure environment so that faculty do not need to worry as much about data loss, and we [the institution] don't need to worry about information breaches as much. They are going to happen, and we need to be prepared for that. We need to take reasonable actions to prevent them. (Kurt Adamson, Interview, 2015, 01:29)

As this institution has recently transitioned to that higher-level IT security role, Douglas stated that it is important to consider what specific qualifications are needed to be successful in a CISO or a security manager role. Douglas stated that:

> The success of the security projects at an academic institution are not as much dependent on whether or not they have a person dedicated to the task and much more on what type of person is working on this. Are the projects presented from the CIO, from someone who used to be a System Administrator and is still heavily versed in the technical realm, or are they presented by someone who has an MBA or a PhD and is really able to translate all of the security projects and the impetus behind them in terms that the audience is able to digest? (Everett Douglas, Interview, 2015, 1/17:13)

Getting that security position to be a higher-level position is one step in the right direction, according to Samuels, Adamson, and Douglas. However, Douglas stated that "security, for years, for decades, has asked for a seat at the table" (Everett Douglas, Interview, 2015, 1/33:08). He continued:

> Now we have that seat at the table and it's up to us [IT and security personnel] to really step up and to be able to speak in the correct language. It's kind of like learning a new language and adapting our sub-patterns to using that language. (Everett Douglas, Interview, 2015, 1/33:15).

Governance and systems.

The following interview questions were asked by the researcher to determine what technical systems, policies, and other frameworks for decision-making were in place at this institution:

- What policies and procedures does your institution have regarding the topic of mobile devices and security of those devices?
- What types of systems do you use to manage mobile devices (example: Mobile Device Management solution (MDM) or something similar)?
- What information does your institution collect about mobile devices and usage by faculty, staff, and/or students?

This institution is part of a larger system that is also supportive of increasing the security of the institution's systems (Kurt Adamson, Interview, 2015; Everett Douglas, Interview, 2015). This can be a positive thing but can also create some conflict if the initiatives are not aligned. For example, this institution's over-arching governing body has adopted a particular security standard that applies to the entire institution's

infrastructure, and the governing body is forcing the institution to comply within a certain period of time. Douglas states that the mandate is problematic for several reasons (Everett Douglas, Interview, 2015, 2/08:12). First, it is problematic because the institution itself had very little say in the entire process, and many of the institution's leaders are not even fully aware of the mandate. Second, it is problematic because the mandate lacks any funding associated with it, and there are no additional resources to devote towards meeting compliance. So without reassigning resources, it becomes incredibly difficult to comply with the complexity of the mandate. Third, the security standard itself is a bit vague, and it is difficult to interpret what exactly 'compliance' means. Fourth, it is problematic because no single standard will fit every institution. Douglas stated:

> There's a lot of potential issues there. Any time you do a mandate like that across such a large institution. We all have such diverse needs and such diverse staffing levels. I can imagine that it would be incredibly hard to comply with some of those things, based on the resources that they have. (Everett Douglas, Interview, 2015, 2/09:44)

Douglas believes it is important for institutions to personalize their security plan and adopt a plan that meets their specific risks and gaps (Everett Douglas, Interview, 2015, 1/08:48).

This institution has a policy that outlines acceptable use of devices but does not appear to have a data classification policy or a specific mobile device policy in place yet (University web site). When asked if there was a specific policy around mobile devices, Adamson replied:

> Not for mobile devices specifically. There aren't any policies, per se, on that. People are guided by things like FERPA, best practices, campus privacy policy. We don't have a formal policy to say what you can and cannot store on your personal device. (Kurt Adamson, Interview, 2015, 04:26)

Adamson further stated that, in their environment, it is difficult to tell the faculty where they can and cannot store data. Adamson stated, “It’s really hard to do in a higher educational institution with faculty having Academic Freedom and really owning their content” (Kurt Adamson, Interview, 2015, 04:47). Faculty may be looking to view or store student contact information which may or may not be confidential depending on what type of data were being stored. They may be looking to view or input grading data or coursework. Staff may be viewing confidential human resources or financial files. The possible uses are limitless. Despite the difficulty, a data classification policy is something the institution is working on today.

From a BYOD support perspective, Jackson stated that the security manager started working on a policy and service level for mobile devices, and that work is ongoing but not complete yet. The unwritten policy is that “we will try to support any device possible” (Luke Jackson, Interview, 2015, 04:01) but Jackson stated that the need for a policy is still there. Jackson stated that it is important to get all parties in agreement but also important to have something written down that IT staff can actually enforce.

Jackson stated that today:

> You almost have to design everything to that lowest common denominator in order to make everything work, and sometimes you are sacrificing security, performance, and maybe supporting other devices well just to be sure that

> everything works, so that BYOD policy and Service Level Agreement is pretty important, and we've just been lucky that we've been able to get by without one so far. (Luke Jackson, Interview, 2015, 05:48)

There is a broad mix of both personally-owned and University-owned devices at this institution, and basic support is offered for all of these devices, though more in-depth support is available. For University-owned devices, this in-depth support is free while this greater support is available at a fee to the faculty, staff, or student for personally-owned devices. For example, a person with a University-owned device may bring their device in asking for assistance if it won't turn on, and the service desk would help them figure out what was wrong. That same service would result in a charge for a personally-owned device. Interviews suggested that it is difficult to provide broad support for all devices because of the vast array of devices that are owned. There is little consistency in device type or system, and this makes it challenging to support all devices.

The institution does track their University-owned assets but does not have one formal mobile device management system that they use for tracking all assets. They utilize a cloud-based e-mail system that has some light mobile device management capabilities, but they have not explored these greatly. Adamson stated that:

> The proliferation of mobile devices has created a significant challenge in security. We don't have a heck of a lot of formal mobile device management. The most we have right now is through [the cloud-based e-mail system]. We can go on [the cloud-based e-mail system] and direct a device to wipe the e-mail. But that's as far as we can go. [The cloud-based e-mail system] is just releasing a more comprehensive mobile device management program. We haven't looked into it yet

> to see what all that entails. But that is definitely something that has got to be on our radar just because of the proliferation of devices. (Kurt Adamson, Interview, 2015, 02:58)
>
> Adamson further explained:
>
> I just read a study last night that said something like 70 percent of people in the work force have allowed company data on their personal device. Now since we talk about information security and talked about data security, that's really concerning because we [Institution A] don't have a way to track that. (Kurt Adamson, Interview, 2015, 03:30)

If the institution is unable to know what is being done with mobile devices in their environment, it makes it difficult to predict the security risks. Employees may be accessing their own pay information, such as salary, benefits, and more, but the true risk lies in the systems they are logging into from their mobile devices and their credentials (username and password). When the employee logs onto the payroll website from their mobile phone, from example, if their username and password is stolen, or compromised, it puts the entire network and all systems for the University at risk. Once a hacker has that username and password, they use that as a gateway to get into other systems and cause further damage to the institution.

Data collected about these devices are available from the network environment and web site about basic traffic and usage, but it is not currently being examined unless a problem is reported. When asked if they collect data about mobile device usage, Adamson stated:

> Not proactively. If there's an incident like a DMCA incident, we will look. We have logs on our wireless network to say what devices have been connected and who authenticated to that device. We can look and see where that device logged in from. (Kurt Adamson, Interview, 2015, 05:49)

Interview subjects indicated that it would require more staffing in order to examine this data. Jackson stated that additional staffing resources are greatly needed in the networking and security areas (Luke Jackson, Interview, 2015, 25:51). The residence hall network is separated out from the main campus network today, and a company provides the Internet service to the residence halls. If students have complaints about wireless or network issues, they are handled by that company directly. Over the past few years, the institution has spent over half a million dollars on their wireless network to address the massive growth in mobile devices, and they are about to spend more to increase the number of access points on campus even further.

As they examine their wireless network, Samuels believes strongly that separating mobile devices on the network can add a layer of security that is critical. Samuels stated:

> In addition to the MDM-type stuff, one of the other things that we need to do, and this will help, is I've asked my team to do further segmentation of our networks. Ideally, we would have mobile devices on a segmented portion of the network where they could access some things but not others; and that would help us greatly with the mobile security stuff at least on campus. (Victor Samuels, Interview, 2015, 11:00)

Samuels explained that “what we’re trying to move toward is, if we know the machine belongs to us, it goes on one network. If it doesn't, it goes on a different

network" (Victor Samuels, Interview, 2015, 20:36). By separating these out, Samuels believes institutions are able to better protect the campus network. This institution is working on plans to do this today because this is a direction Samuels feels strongly about going in the near future.

Institution A does have a small implementation of an MDM for iOS devices but has not adopted another option for other types of devices. Jackson states that these solutions are difficult to implement because of the high cost, both in dollars and resources, as well as the rather vocal resistance from faculty about tighter controls on their mobile devices. "Most of the faculty understand that their mobile devices are state property, and they are okay with that, but they don't want to be watched, and they use Academic Freedom as a reason" (Luke Jackson, Interview, 2015, 08:40). Samuels stated that the MDM that the campus is using for iOS devices is limited in usage. It has less than 100 devices connected to it, but they know there are many more out there (Victor Samuels, Interview, 2015, 06:03). According to Jackson:

> The big problem with all that [mobile device management systems] is number one the cost of it, and then the second thing is getting acceptance from people that we're going to be closely managing their devices. We anticipated that we'd get some kick-back from faculty on that one, so between the policy and getting everybody on board with, "Hey, this is the reason why we're doing this" and then the question of who's going to pay for it. Because some of those mobile device management solutions are pretty spendy. (Luke Jackson, Interview, 2015, 7:40)

When discussing the difficulties in implementing an MDM, Samuels cites the fact that personally-owned devices are in the mix along with University-owned devices as

being a large challenge. When referring to the personally-owned devices, “getting people to enroll is actually quite a battle. You know, you’re not going to -- people don’t voluntarily give that up” Samuels stated (Victor Samuels, Interview, 2015, 08:50). Jackson stated that he thinks “that deep-down people feel a sense that it is their personal device, and they can do with it what they want” (Luke Jackson, Interview, 2015, 8:50). Jackson stated:

> We have a lot of faculty and staff too sometimes that bring their personally-owned devices, and they use that for class. They might have an iPhone that they use for a lot of school business, and they don't want you to put stuff on there to manage and watch what's going on. So there is that little bit of mistrust. On the other hand though, they want to shift the responsibility to making sure that everything is patched and everything is going okay and working fine, they want to shift that back to IT. So they kind of want to do that but then they don't want it to at the same time. (Luke Jackson, Interview, 2015, 09:00).

Despite wanting to retain control, Jackson feels that their faculty often still expect IT to make sure their technology is secured, so it is an interesting balance to make sure devices are secured without being too intrusive.

Douglas believes that largely faculty are not very aware of what is possible to do through the cloud-based e-mail system that the institution is using. He also believes that they are unaware of the fact that this system has the capability to remotely wipe their entire mobile device at the push of a button. Douglas stated:

> This is, I think, something that a lot of IT shops are doing, where they are not even realizing that a lot of the controls they have in place that are not preceded or

> supported by governance pieces or policy pieces; which can put them in a lot of trouble. But once I found out we had an MDM, I said, "Well, let me test this thing." And so I had a spare device. It was a tablet. I registered the device with my e-mail account and then I went into the ActiveSync system, and I said, "Hey, let me just go into a remote wipe on this device." And then, within less than five seconds later, the device started completely shutting down and doing a full reset. And to me, this was horrifying. (Everett Douglas, Interview, 2015, 1/22:27).

Douglas mentioned that by employing a solution like this without communicating first, institutions have missed a critical step.

Samuels agreed that even though faculty and staff sign an agreement outlining the controls the institution has on their mobile devices the moment they connect to e-mail, he has witnessed firsthand that some people are still unaware. Samuels related a story from a recent meeting he had attended where discussion arose around IT having the power to remotely wipe their mobile devices:

> I reminded them that we already have that power. And some of the faculty were clearly -- they said, "You can -- you can wipe my phone?" I said "Absolutely. You signed an agreement to that effect." (Victor Samuels, Interview, 2015, 25:50).

Despite the signing of the agreement, Douglas, a faculty member, was clearly unware and stated:

> As a faculty member, nowhere in my institution’s communication has it been made clear to me that if I don’t go out of my way to save the data and the pictures and whatever else I might have on my own device, that the moment I hook it up to

> the e-mail system, that suddenly it's possible for the institution or even someone else who has access to my username and password to initiate a reset. (Everett Douglas, Interview, 2015, 1/23:45)

This is very concerning for those interviewed because they all agreed that faculty should be aware of what is happening to their devices when they choose to connect to e-mail.

At the time of this study, this institution was about to perform a security audit brought on as part of a larger initiative by their over-arching governing body, and Samuels was welcoming the audit with both arms open. He stated "I volunteered us to be one of the first as it really helps with the education and the security initiative" (Victor Samuels, Interview, 2015, 09:55). Samuels believes that a breach is not a matter of *if* a breach occurs, but a matter of *when* a breach occurs for most institutions. Samuels stated:

> Security, right now, is built around that you build walls around your stuff. And then, you hope that the bad guys don't get in. And that model of security is just never going to hold up. I mean, it's always going to fail somehow or another. So it doesn't really matter how well you do security. If you're a healthcare company, if you're a financial company, if you're a University, you will be breached at some time. And we're seeing that play out right now across the world, breaches all over the place. (Victor Samuels, Interview, 2015, 11:55)

The findings from the audit assist the IT department in improving security in the environment, as well as making a stronger case when going to the administration and to the larger campus community asking for participation, security changes, or additional resources.

One of the main ways to obtain campus buy-in on security initiatives is by increasing communications to faculty, staff, and students. Samuels stated that he is using the audit as a way to have more of those conversations. He stated:

> I actually am doing listening sessions with each of the colleges. I did two of them yesterday. I'm doing two more today. I have two more next week. And then, you know, with the meet and confer process, so this is just informing the entire campus, along with our technology governance body that, “Hey, this audit is coming. We're going to have to change our behaviors.” Some of it will result in some inconvenience, and we have to decide where we want to be as a University, what level of risk we're willing to assume and what level of risk is unacceptable so that everybody is on notice. (Victor Samuels, Interview, 2015, 10:15)

Samuels sees this as a partnership where IT needs to be communicating with the campus community and helping the governance body make decisions about what risks should be addressed and how much funding is needed to remediate those issues.

In keeping with the theme of partnership, the institution has developed a plan, or roadmap, for security in coordination with campus. Samuels feels that it is important that the security roadmap or plan integrates with the strategic plan for the IT department and for campus. Samuels stated:

> It's a standalone plan, but it ties together with our [the University’s] strategic framework. It is built off of the SANS Top 20 Controls. So the plan is, I guess, very specific in terms of the top twenty most common areas of compromise. And, if we address those problem areas, we address over 95 percent of all possible breaches. (Victor Samuels, Interview, 2015, 16:40)

By utilizing the SANS Top 20 Critical Security Controls as a baseline, it allows them to focus their resources on the highest-target areas first.

Taking that one step further, after selecting the SANS Top 20 Critical Security Controls as their base framework, Adamson stated:

> We were audited against the SANS Top 20 Critical Controls, along with a few other institutions. I do not have that report yet. So that report gives me a baseline. That report will give me a baseline of where we're at. And then I will be able to go from there and say, "Okay, here's where I'm at today. Here's where I need to be in the future. How do I get there?" (Kurt Adamson, Interview, 2015, 14:05)

However, as the institution seeks to address some of the security risks, there can sometimes be a trade-off. All of those interviewed mentioned the struggle between access and security. Things that increase security typically reduce access, and that can be problematic for faculty, staff, and students who are trying to use technology to reach their educational goals. Jackson stated:

> Being in the education environment, what we have really always focused on is trying to make everything that somebody might want to use work in our environment as easily as possible. It's actually been an easier goal to achieve lately because of the better quality devices, better software, better drivers and things like that where it came in in the large Cisco wireless environment. So what we've been trying to do on the network side anyway is make it so that anything that you want to use on our network will work. What's been lagging a little bit is the support for those devices. (Luke Jackson, Interview, 2015, 00:57)

When asked what led him to the conclusion that more support was needed, Jackson stated:

> The strongest or the most vocal drivers were faculty bringing in devices and expecting them to work well, but the sheer volume of need was the student side. (Luke Jackson, Interview, 2015, 02:42)

Further describing the problem, Jackson stated:

> We would get people stopping by the service desk if devices weren't working. They couldn't authenticate. They couldn't use the wireless networks or if they were not working reliably or we would share things in meetings or they would complain to faculty and faculty would complain to us [IT staff] that things weren't working well. So it was kind of coming in from all directions. (Luke Jackson, Interview, 2015, 03:09).

Recognizing that, the IT department requested additional funding for staffing to assist in the support of these mobile devices, and their request was granted. Jackson stated:

> We were able to actually get some more funding to do a better job of supporting all devices on campus. So now our support is kind of in line with the goal of Bring Your Own Device which is working out pretty well. (Luke Jackson, Interview, 2015, 01:57)

He explained that reaching the goal of increased support and access for any device someone wants to use has been easier because they have these additional resources and also because devices have become easier to use and manage. However, there are still more needs for security than staffing to address them.

When asked about faculty and staff perception of mobile device security, Jackson stated:

> They just kind of assume that we're taking care of all that, and nothing is going to happen, and everything is safe and secure on their devices. So from their perspective, they just want it to work. I think, the perception is if you have Internet service at home, I think the perception for most people is probably the same, that whatever carrier you have, they're providing proper protection for you. But in reality, they don't block anything coming in, so if you want protection on your home network, you have to patch your own devices, and you have to put in your own firewall router. A lot of people don't realize that they're susceptible. They think they're protected, but they're really not. (Luke Jackson, Interview, 2015, 28:21).

Jackson brings up the important point about how mobile devices make it easier for employees to work from home or work from anywhere off-campus, but doing so is a security risk for the institution. Individuals must secure their own home network, but many do not realize this, and this can present an additional risk when they are accessing institutional data from their home location. When traveling off-campus, faculty and staff connecting to any network they encounter that may or may not be secured is also a risk. Today, there is little data about what faculty and staff are doing off-campus with their mobile devices, and so the extent of this problem is largely unknown. When asked about faculty, staff, and student usage, Jackson stated that, “We don't track it too closely” (Luke Jackson, Interview, 2015, 11:46). Jackson also feels that resources are a problem and stated:

> The problem that we have with our network environment right now is we only have two guys that can do that, and they are completely overwhelmed. We need a third person and over the past year have been unable to add that person that can focus on security and better management. So right now, we're just completely strapped by resources. (Luke Jackson, Interview, 2015, 12:10)

Because this problem is largely unknown and resources are limited, much of the focus has been placed on what can be done on-campus to increase security. In the past, the IT department has explored using a system that only allows certain devices on their network if they pass a set of security tests, such as whether they are updated, running anti-virus, et cetera. However, after reviewing those products, the feedback they received about these types of systems is that too many devices do not meet those standards, and this greatly inhibits the business of the University. It creates a massive barrier to students being able to complete their coursework. Jackson stated:

> We've been looking at it for many, many, many years, probably the last 10 years, and the theory is really good that you have to have a device that's patched and anti-virus is running on it. You have to pass all these levels of tests to make sure that your device meets policy before it works on the network, and that's a really good theory. The problem that we've had with it, though, up to now is that you have to download a client, the device has to be patched, and you have to go through quite a bit of maintenance work in order to get it on the network. In some cases, that can be a huge barrier for students sitting down in a classroom, and then their device doesn't work on the network. We've talked to a lot of people about that, and we've found that really people will get extremely frustrated at IT because

> their device doesn't work. We've talked to a lot of schools too that have done this, and they said that they get beat up pretty bad because the class sits down, and half of the devices don't work on the network. Faculty get really frustrated that they have to sit and provide tech support for the first 15 minutes of class to try to get all these devices working. So we knew that was not going to work at our school at all. (Luke Jackson, Interview, 2015, 31:57)

Jackson further states that though this would significantly improve security to the environment, this would put a major drain on their staffing and would simply not be successful right now with current staffing levels. He stated:

> Our security guys think that is definitely the way to go, and I think we would really like that. We would like all the patches applied on devices before they get on our network. But we've found that that just won't work in our environment. (Luke Jackson, Interview, 2015, 34:03)

Increased budget is needed, according to both Jackson and Adamson, to assist with improving security at this institution. When approaching the administration to request this additional funding, Adamson states that a key step is:

> Positioning it [the proposal] in such a way that it makes sense to them. Positioning it as a priority for the University. It's going to be part of our overall information security initiative. (Kurt Adamson, Interview, 2015, 13:20)

Adamson, Douglas, and Samuels believe it is critical that the CISO look at it from a business perspective and speak in terms that are understandable and relatable by the upper administration and not in IT language. Adamson stated that “part of what I'm working on right now, as I'm fairly new to this role, is my information security strategy”

(Kurt Adamson, Interview, 2015, 13:45). The funding needs to be a part of the overall security initiative, which is currently being developed at this institution.

Future plans and trends.

The following interview questions were asked by the researcher in order to determine the interview subject's perspective on the direction of mobile device security, both at this specific institution and in the industry at large:

- What trends do you see coming in the future regarding mobile devices and/or security?
- What do you think your institution does regarding the security of mobile devices that needs improvement?
- What resources, processes, policies, et cetera do you wish your institution had to assist with the security of mobile devices?

Adamson stated that mobile devices are a growing segment of technology, and the greatest challenge in the future is securing the personally-owned devices as well as those University-owned devices. Adamson stated:

> Trends I see is just the continued proliferation of mobile devices. I see mobile devices becoming an even bigger security target, just because there isn't, even industry wide, there isn't a lot of mobile device management. And I haven't seen a clear winner as to a mobile device management vendor. There's a lot of them out there now, but I imagine that space will get tighter. Mobile device management is going to become a priority, probably within the next year or two. As I think about my personal smartphone, if I were to lose that, I don't have any confidential data necessarily on there, but I've got a lot of things that I don't really want people to

> find. Anything like that kind of gives the University a black eye. (Kurt Adamson, Interview, 2015, 10:22)

Trends that Adamson has seen for the future include trying to delineate between the personally-owned devices and University-owned devices, which would enable an institution to evaluate a personal device and limit it to a specific portion of the network and restrict it from the larger University network, thereby keeping the University network more secure. When asked if they delineate between devices today, Adamson stated:

> We don't. I'm hoping to in the near future. I'm hoping to be able to delineate enterprise versus BYOD. (Kurt Adamson, Interview, 2015, 21:46)

He continues:

> It will provide us with the ability to segment our network, based on device type, based on security profiles. I don't know that we'll actually get to this, but in theory, we'll be able to evaluate somebody's personal device, and say, "Okay, yeah, we're going to let this on the enterprise network," versus just the public side of the network or the student network. (Kurt Adamson, Interview, 2015, 22:02)

Adamson stated that mobile device security is "just like everything else in security, it's a growing segment, and the challenge is going to be how we secure personal devices versus enterprise devices" (Kurt Adamson, Interview, 2015, 21:24).

In talking about how to stay up to date with trends in security, Samuels feels that peer networking is a critical component. Also, seeking out the computer science and security experts within the faculty is an important piece of the puzzle. When asked how he stays current in mobile device security, Samuels stated:

> We're part of the REN-ISAC list. We're members in that. And then, also, obviously, attending conferences, making sure that my staff gets trained. You know, ultimately, I'm responsible for the IT security; but I have a Chief Information Security Officer-type position on my campus. And that position's job duties are to keep me informed and keep the campus informed and keep us up to date with an information security plan so there is a goal for that. (Victor Samuels, Interview, 2015, 14:41)

Samuels suggested that reaching out to these faculty members can create a richer security program, ensuring better planning for the overall campus, as well as assist with getting buy-in from other faculty members. Each of these connections help the institution adjust as new threats and new capabilities are developing in the industry.

The next wave of technology, according to Samuels, is stealth technology. Samuels stated:

> Instead of trying to draw a wall around the access, basically hide the access so they’re invisible except when people need to – so the access is just not there until it needs to be accessed” (Victor Samuels, Interview, 2015, 13:00).

This development is not mainstream today, however, and not something that’s ready for mass adoption quite yet.

In the future, Adamson explained that he sees a continued growth in mobile devices as a security target (Kurt Adamson, Interview, 2015, 10:22). Because of the fact that mobile devices will be an increasing target, Adamson stated that “mobile device management will become a priority within the next year or two” (Kurt Adamson, Interview, 2015, 10:45).

One trend for the future that Douglas believes is important to consider is where the IT security personnel live in the organizational structure of the institution. There are times in the private sector, Douglas states, that IT security does not even live within the IT department at all; furthermore, having it do so could even be considered a conflict of interest. “An increasing number of CISOs are housed in places other than under the CIO,” says Douglas (Everett Douglas, Interview, 2015, 1/19:23). Douglas stated:

> They might be put under the CFO. I've noticed a CISO who was reporting directly to his CEO for a while. In some cases, they're put under chief risk officers or even legal. And so that creates different lines of communication and reporting, and so that structure is key in a way, that governing structure, that organizational structure. (Everett Douglas, Interview, 2015, 1/20:00)

The IT perspective can sometimes conflict with the business side of the house, and having security under IT can mean that security initiatives may take a back seat to a larger IT initiative. Douglas suggests that institutions should not automatically assume that the IT security roles should live within the IT department. It is important for institutions to first look at the goals and align the organizational structure to those goals.

In addition to the question of where IT security staff should live in the organizational structure, there is also the question of obtaining qualified candidates for security roles. Douglas indicated that one of the largest problems facing IT security departments in the realm of higher education is obtaining the competitive salaries that are necessary to hire qualified candidates. Douglas stated:

> Our institution has gone through, just in the past three years, we've had three different security manager-like positions. So one person left to go get, well,

> actually both people before the current one had left to go get better jobs. Part of it is the salary structure within the system, and specifically in higher ed in general, the salaries are not keeping pace with what's out there in the industry. (Everett Douglas, Interview, 2015, 1/18:24)

The IT security positions, even non-management positions, in the private sector are frequently found to be making six figures because of the highly specialized nature of the field. However, in higher education, the salaries of IT workers typically lag behind those in the private sector, and this is much more keenly felt with IT security jobs where the gap is the greatest, according to Douglas. Without the ability to offer a competitive wage, higher education institutions run the risk of losing the skilled security employees that they have today and of not being able to attract new qualified candidates in the future.

However, Douglas stated that:

> Even when IT management is on board and trying to be supportive, sometimes they still don't fully grasp the ramifications of the security realm in a way. I've met a number of CIOs who have basically pointed out that they think they own all IT risk, which from my perspective was just a big no-no. (Everett Douglas, Interview, 2015, 1/08:48)

Douglas pointed out that this is a common misperception, but that IT risk is actually owned by all aspects of the institution. Security is everyone's business, Douglas specified, from the Board of Directors to the President to the CIO and on. Douglas suggests that one physical way of altering this mentality that security risk is solely the IT department's problem is by having the IT security staff members report outside of IT.

In a positive turn of the tide, Douglas stated that the conversation has shifted, and upper administrators such as CEOs and CIOs are now asking a different question than previously asked. Douglas stated:

> For a long, long time, the conversations of executives and CIOS or executives and CISOs, when CISOs were allowed to talk directly to executives, was “are we secure? Yes or no?” Instead, the conversation has really shifted towards, “well, what is our risk and what are we doing about this?” Because this idea of security is not at all binary. It’s all these degrees of security, and it really depends on what’s going on in the world today. (Everett Douglas, Interview, 2015, 1/29:44)

Douglas stated:

> I think, by now, IT departments within academic institutions are finally waking up to the fact they can't be a “no” shop saying, "No, no, no, no, no," all the time, because, otherwise, they get bypassed, and then they have to play catch-up because somebody signed a contract to leverage something in the cloud, and then they have to try to stop that. Good luck on that. I think they finally got that message of working with the various units. The problem is now we're getting to the “Internet of Things” and we're getting to things where we might not even realize there's an IP address in the Barbie doll that's now got a microphone and recording everything that a kid is saying and then uploading that to the cloud so it can be transcribed and then instructions sent back to the Barbie doll saying, "Hey, move your arms," or something. (Everett Douglas, Interview, 2015, 1/31:00).

Douglas stated that now institutions are realizing they have to work with some of these things, but there are so many advancements happening so quickly that it can be difficult to predict all of the risks.

Douglas believes that the question of who owns the risk is an important one. He stated:

> When presenting in my class, he [a presenter] asked, “Who owns the risk?” Some of the students said “CISO” some said “CIO.” He kept shaking his head “no, no, no.” So he said, “It’s the CEO.” And I had a discussion with one of my students later on, who's much of a techie rather than a business-minded person, and he was like, "I still don't get it." I said, "Well, think about who owns the data. It's still the business unit that owns the data." IT is much more of a custodian. (Everett Douglas, Interview, 2015, 2/01:18)

Douglas stated that this confused the students, and so he explained further by saying that it is IT’s job to take care of the data, but:

> At the end of the day, it's still not our [the IT department’s] data. Just because we can look at it and do things to it, it doesn't mean that it's the right thing for us to do. So, since we don't own the data - we, meaning IT - and the business still owns the data, the business side still owns the risk. (Everett Douglas, Interview, 2015, 2/01:18).

In the example of higher education, this means that the President, as the CEO of the institution, owns the risk. This is important because security is an unseen problem, and one that can easily be ignored until it is too late and a breach occurs. Having the President know that he or she may be held accountable for a breach can create more ownership at

that higher level, meaning that the President will be more willing to listen to security risks, take them seriously, and allocate funding and resources for important security initiatives.

Overall, all interview subjects agreed that mobile device usage at this institution will grow well into the future and that this trend of growth shows no signs of stopping. Because of this, Adamson stated that addressing security risks is “going to be a matter of budget priority, is really what it's going to come down to” (Kurt Adamson, Interview, 2015, 11:34). Adamson stated “with any mobile device management solution, we're going to have to sign off some budgetary money to implement something” (Kurt Adamson, Interview, 2015, 12:45)

When asked how to obtain that budgetary support, Adamson replied:

> It's going to be awareness at the administrative level. Positioning it in such a way that it makes sense to them. Positioning it as a priority for the University. It's going to be part of our overall information security initiative. Part of what I'm working on right now, as I'm fairly new to this role, is my information security strategy. "What do I want to do? How do I want to proceed with information security? What initiatives do I want to tackle first? What's the most important initiatives?" And then talk about what initiatives come next. (Kurt Adamson, Interview, 2015, 13:20)

In order to properly address security, funding is a critical need for the future. When discussing the areas of improvement for their institution, Jackson stated:

> We don't monitor as well what's going on on our wireless network as we're more reactive, and a large part of that is just strictly staffing. We don't have adequate

> staffing for proper security and to really watch what's going on. We've been on other campuses before where we've tried to get on the wireless network and we've tried to do some funny things just as we've been visiting with IT staff, and within a half an hour, somebody will show up and say, “Hey, what are you doing?” We've had vendors too that have come in and said that they've done the same thing. So some places, we really admire that they watch things pretty closely, and we're not able to do that. (Luke Jackson, Interview, 2015, 25:51).

Samuels agrees and stated that “We're very reactive in that area as opposed to proactive” (Victor Samuels, Interview, 2015, 20:27) Both Samuels and Jackson want to move into a more proactive mode where they are monitoring what is going on and responding before incidents are reported, but they simply don’t have enough staff to do that today.

Communications and training.

Though no specific interview question was focused on communication or training, this arose as a theme from each interview. All of the interview subjects indicated that, as mobile devices become more and more prevalent, communication is an increasingly important factor. Samuels stated that “one of the trends across the county, not only in higher ed, but almost everywhere, is this BYOD trend” (Victor Samuels, Interview, 2015, 02:35). Douglas stated that he sees the organizations that are the most successful at securing their environment do not isolate the conversation about IT security to just the realm of IT. Douglas recommends making sure that the IT conversation happens at the administrative level and happens in the right language.

Samuels stated that:

> In terms of mobile security, bring your own device is a trend that I think is here to stay for a while, quite a while; and so the goal is to allow users to access what they need to access but also to make sure that, as they're accessing resources, that it's in a protected way and that, if they lose their device, that you can do something about it. (Victor Samuels, Interview, 2015, 03:00)

Douglas suggests that a first step towards beginning to create a security program that includes mobile devices is a gap analysis, and it is critical to have the entire campus involved in this process. Douglas stated, “These days with things in the cloud and BYOD, these types of gap analyses are critical” (Everett Douglas, Interview, 2015, 1/05:33) When discussing his expert opinion on what makes a gap analysis successful, Douglas stated, “Instead of just doing technical audit-side things, we also build in interviews with the user side of things” (Everett Douglas, Interview, 2015, 1/04:45). Douglas recommends that meetings should include both IT staff and non-IT staff in order to get a true sense of the strengths and weaknesses of an organization.

In order to help inform users, when configuring e-mail on their mobile device, they are asked to agree to a set of controls that require a passcode and says that the institution has the ability to remotely wipe the device clean. Having them click to agree with these security standards helps inform the faculty and staff about what types of control the institution has over their device and their data. Samuels stated that:

> The most common usage that people have for the mobile devices, at least on our campus, is they want to access their campus e-mail and their calendar. And so we require users that access our environment to sign an agreement that we have the right to erase that e-mail on their devices if they lose their device so that the work

> data is not available to whoever gets the device. (Victor Samuels, Interview, 2015, 04:23)

Samuels believes faculty and staff are largely unaware of mobile device security in general and stated:

> I would say, first of all, they're not focused on mobile security at all. They basically almost don't care about it, and they've been unaware of it. In fact, as I reminded them yesterday, what I'm seeing is "What? You can do that?" So I don't think they are aware of it. They think of security as computers, laptops, desktops. They don't think about their mobile phone being part of that (Victor Samuels, Interview, 2015, 30:10).

However, these devices present some of the largest risk to the environment because they are so diverse, and Samuels stated that:

> As these apps pop up that people can download and install and run, there is a high possibility that compromises will arise in this area. And it will be invisible to us until too late because the app ecosystem just grows so rapidly; and you don't have any control over it. (Victor Samuels, Interview, 2015, 30:26)

Samuels indicated that there are many end user educational programs hosted by the central IT department to assist in training faculty, staff, and students. Samuels stated:

> We've done a lot of campus user education. We have these training programs, ranging from your passwords to what networks to watch out for, watching out for open networks, that kind of stuff. We go through the meet and confer processes. We have a couple of technology days per year, and we set up training sessions in

> those areas. I mean, those are just some of the things we're doing. (Victor Samuels, Interview, 2015, 06:55)

Keeping the campus community informed about breaches at other schools can also be a way of helping faculty understand the importance of added security and increase buy-in. Samuels stated that once a breach is publicly known, it becomes an opportunity to prevent that same breach on your own campus. He stated:

> Once the information becomes public, absolutely, I absolutely use the Target breach and the healthcare breach. I use that to my advantage to promote security on campus. I say, "Look what just happened. And Target has way more resources than we do, and they're probably doing the best they can; and we can never even get there. But we don't want your data to be breached this way." It's my job to ensure the environment is as secure as possible. So, yeah, I leverage it. (Victor Samuels, Interview, 2015, 27:00)

When discussing the largest point of weakness at the institution, all interview subjects cited end users as the number one risk to their institution's mobile device security. Samuels stated:

> It's really basic user practices, basic user education. You know, we run the training. But I have people on campus that I know we have told over and over again not to do X, Y, or Z. And in a couple of days or a week, they potentially compromise themselves, their machines, or whatever, just because that's the weakest link. (Victor Samuels, Interview, 2015, 18:10)

Douglas indicated that often security is viewed as a barrier to being able to complete one's work. Douglas stated that sometimes people feel that:

> Security only gets in the way. Instead we [IT professionals] need to say security is part of the way that we do business, and we have to learn to better communicate, to better integrate, so that it doesn't end up being something we try to bolt on in the end and no one is happy with it. (Everett Douglas, Interview, 2015, 1/09:10)

Douglas stated that often faculty "complain very loudly and very quickly" and sometimes IT leadership were fearful of this and did not undertake specific security initiatives because they knew the faculty would be resistant (Everett Douglas, Interview, 2015, 1/09:40). Balancing the usability with the security is an important part of the picture. An example of this is with passcodes being forced to be used via the University's cloud-based e-mail solution. Douglas stated:

> About a year ago, they set out to push a policy update to enforce screen locks, screen savers with password locks, and when they presented this to faculty union, they really were not prepared for the amount of pushback they got. They actually had to basically table their plan to deploy this and come back and really explain, why are they doing this? What is it that is going to help mitigate in terms of risk? What are the exception policies? Because, initially, they hadn't planned for much of that. And, to me, that's very representative of this disconnect and this idea that we really don't want to make faculty angry. (Everett Douglas, Interview, 2015, 1/10:27).

Planning and communication needs to include the reasons for the change, what security risk are they mitigating, what is the exception policy for those that it will not work for. If all of those elements are included in the communication, the resistance will be much less.

Preparation is key, according to Douglas, as well as frequent communication with the faculty. Higher education leaders need to think about how they are going to present their case. Douglas stated:

> Even today, even with the thirst, even with the demand from the higher-ups -- the executives getting the same message that security is important, but it still has to be sold as a concept. Now, the difference is, faculty members and usually folks in higher-ed are very data-driven. If you give them the facts and you say, "If you don't put on your seat belts when you're driving your car and you get in a wreck, your chances of survival are very low." And so, you can gather the facts and then present things to them in a very matter-of-fact way, and my personal belief on that is you can make faculty members or you can get them to really see the reasons why. And that's usually the piece where I believe a lot of the IT shops really don't take that as seriously, and in a way, we're technologists. We love that kind of stuff, and we don't understand how come people are not on board with this. Why is it that it's going to be an inconvenience for you to have the screen saver come on automatically every five or ten minutes while you're trying to teach something? Okay. As long as we make the case, as long as we make partnerships, and I'm sorry here I keep saying “we.” And when I say “we,” I actually shift roles. So, sometimes I say “we” and I mean “we” as faculty, and sometimes I say “we” and I mean “we” as technologists. But it would be much more advised for technologists to really partner up with representatives from faculty and other groups to be a sounding board to get some feedback before they start launching

> some kind of change because people are reluctant to change, and faculty members are super reluctant to change. (Everett Douglas, Interview, 2015, 1/11:51).

Douglas believes that if you show faculty the reasons why you need a particular security initiative or change, this will tremendously increase buy-in on security initiatives.

Adamson agrees that whenever launching a new security rule or policy, it's important to let faculty and staff know why the institution is making the change. This not only increases the likelihood that they will comply but can also decrease complaints and increase the buy-in on the change. Adamson stated, "If I can tell them how it impacts them, they are more likely to do it" (Kurt Adamson, Interview, 2015, 17:15).

Adamson stated that any conversation with faculty and staff around the security of mobile devices has to be in terms that are relevant to them. Adamson stated that:

> They don't want to have to think about it. They just want to be able to do their work, teach classes, and not have to think about mobile device security. We need to make it as transparent as possible. (Kurt Adamson, Interview, 2015, 20:23)

When asked how important communication is when implementing a security plan at an institution, Douglas stated, "I think it's nearly all of it" (Everett Douglas, Interview, 2015, 1/15:53). Throughout his entire interview, Samuels also articulated strong support for robust communication plans. Both Douglas and Samuels believe that communication is critical to a successful security initiative, and Douglas further clarified that institutions need to be:

> Thinking about the disruption this is going to engender in our audience and making sure to structure the message in such a way that it's going to be received in as positive a way as it possibly can be. Even if there is already support from the

> President of the institution, it’s still a change, and that change has to be, it’s like taking a big pill or something, it has to be coated so that it’s easier to swallow. (Everett Douglas, Interview, 2015, 1/16:00)

Adamson stated that:

> My first line of defense in security is awareness, making people aware of how their actions impact their life, how their actions impact the University. I wouldn't say that I even follow security standards on my device, just because I haven't gotten there yet. But being aware of, okay, if I lose my device, what is it I'm going to lose? What data's going to be lost if I do that? Not to tell them, "Don't do it," but just so that they're aware. (Kurt Adamson, Interview, 2015, 12:00)

Adamson believes that being aware of what happens when a person loses a device can go a long way towards assisting in securing the environment, preventing that loss in the first place, and handling it properly once it occurs.

When asked what is needed to help make a security awareness program successful, Douglas stated:

> If we had security awareness, security education campaigns with goals saying, okay, in a year's worth of time or three years' worth of time, we're going to spend a little bit of time talking about credit card safety and machine safety and mobile device safety and username safety and password safety. And instead, it's very much like scatter shots. Hey, Joel from the tech sector here, we're going to go and make you responsible for the next three to six months for the next awareness campaign. And so, here come the posters and the scary stuff and the pictures of

> skulls and bones and don't do this and don't do that and don't do this. (Everett Douglas, Interview, 2015, 1/24:41).

The IT department at this institution trains help desk staff to answer basic questions about mobile devices but they do not have trainings unique to security awareness at this time. There is a data privacy course that all faculty and staff are required to take as part of their employment, and there is information on security on the ITS web site. Douglas feels that training programs at many institutions today are too haphazard and not consistent. An institution makes a big push during a specific month or when a new policy is launched, but there needs to be something consistent and ongoing. Douglas is currently examining how to make security training more effective, and one of the things he advises is that institutions do not focus on the negative. Douglas believes a plan is imperative to the success of the initiative as well as a positive message. Douglas stated:

> One of the items that's grounded in experimental psychology is when you tell people don't do something, one of the first things they're going to do is do it. In terms of getting the message across, it doesn't work as well as positive framing. (Everett Douglas, Interview, 2015, 25:35)

Douglas recommends that institutions give training that focuses on tips and proactive things that end users can do to assist in making themselves more secure. Many faculty and staff want to know what actions they can take to protect themselves, and if IT frames the training in this positive voice, Douglas states that research shows improved retention of this information.

Case Study #2 – Institution B

Introduction.

Institution B is a large institution, granting both undergraduate and graduate-level degrees. It is located in the central United States with over 30,000 students and employing over 15,000 people (University web site). The institution is widely distributed, occupying multiple campus locations. Educational delivery includes face-to-face, online, and distance instruction using a wide variety of methods and tools. Because of the size of the institution, there are a massive variety of services, ranging from a centralized to decentralized IT structure and every combination in between. The interview subjects, Duncan Brooks, Matthew Hudson, and Kyle Lawrence, work in various IT roles across the institution; two in central IT and one in a decentralized IT department.

Environment and staffing.

The following questions were asked by the researcher to assist in creating a picture of the environment at this institution:

- Please describe the role you take in working with mobile devices and/or security at your institution.
- What do you think the perception is of the security of mobile devices by the faculty and staff?
- What do you think your institution does well regarding the security of mobile devices?

Though IT support at this institution is extremely decentralized, there are some functions that are centralized for certain areas, such as basic support and help desk services. Kyle Lawrence stated that his department made the shift to have the central IT

department provide more of those basic technology support services, including the security that goes along with those services. When talking about basic technology support, Lawrence stated:

> That shifted to central IT last year. We did that for a couple of reasons: one, budget-wise, the college had a pretty tight couple of years there; and, two, because that shift of moving away from the people that fix the computers allows us to get a different relationship with the faculty, students, and staff. (Kyle Lawrence, Interview, 2015, 01:30)

Brooks stated that many folks are calling the central IT service desk for support. When asked about the top issues related to mobile devices, Brooks stated that they are calling about “getting connected to their mail and calendar, or getting connected to our wireless network” (Duncan Brooks, Interview, 2015, 01:12) Processes around these types of support are documented and appear fairly well established. When asked if users are informed that they have the capability to remotely wipe their device, Brooks stated that:

> We have some of that in our setup instructions. Why we're doing it, if you're in this space, this is what you have to do and why. But we don't make them sign an agreement or anything. The way we've handled that is if they actually call us and say, "Hey, I lost my phone," then we have that conversation with them. "Well, did you? Okay. Then we're going to have to wipe it." Usually on the newer devices, it's become less of an issue because they have so much automatic backup stuff built in also. That’s a different risk because it potentially is backing up our stuff somewhere else too (Duncan Brooks, Interview, 2015, 04:40)

As long as a phone has been hooked up to the institution’s cloud e-mail system, it can be remotely wiped. All it takes is for it to connect to the Internet, either via a data plan or wireless Internet connection. No additional software is necessary to install on the mobile device to enable this capability.

Explaining the process further, Brooks stated:

> Generally, they call the service desk, and we have a process in place to help them wipe their own phone. If we have reason to believe that it wasn't just an, "Oops! I lost it,” someone is targeting them, then we do have a different security office that would do risk assessment and response. You know, "What did you actually have on the device? Was it encrypted?" those kinds of things to evaluate if we need to do a brief notification or anything along those lines. (Duncan Brooks, Interview, 2015, 05:44)

If a device is lost or stolen, there is a process to escalate the issue to the central security team to deal with reporting the device as lost, remotely wiping it if necessary, and other processes that need to be completed to ensure University data are protected.

Though these items are handled by the central IT service desk, Hudson, a member of the central IT department, stated that “everybody has security in their role” (Matthew Hudson, Interview, 2015). Hudson further explained that is important that everyone has security as a mindset but still critical to have an entire team dedicated towards security as well. As the decentralized service areas move towards dealing more with faculty, research projects, and innovation in their particular specialization, this makes it even more important that the central IT department take ownership over the security

coordination in order to ensure cohesiveness across the institution (Matthew Hudson, Interview, 2015).

Individuals interviewed indicated that the institution has a good focus on IT security, and the IT security department staff employee numbers have nearly doubled in size over the past ten years, from just over ten to approximately twenty staff members dedicated to IT security with a CISO position overseeing this entire area (Matthew Hudson, Interview, 2015). Over that same period of time, Hudson indicated that the University has moved from an approach that was primarily reactionary to one that strives to balance proactive measures to prevent security issues while maintaining the ability to react to incidents that occur with the appropriate measures (Matthew Hudson, Interview, 2015).

Governance and systems.

The following interview questions were asked by the researcher to determine what technical systems, policies, and other frameworks for decision-making were in place at this institution:

- What policies and procedures does your institution have regarding the topic of mobile devices and security of those devices?
- What types of systems do you use to manage mobile devices (example: Mobile Device Management solution (MDM) or something similar)?
- What information does your institution collect about mobile devices and usage by faculty, staff, and/or students?

This institution does have a clear data classification policy that is communicated across campus and on their web site. Hudson stated that this was the first step necessary

before undertaking any additional security initiatives because they had previously only had two groups of data: public or private (Matthew Hudson, Interview, 2015). In today's environment, Hudson explains, there are more needs, and trying to control all data at the same level as HIPAA data was incredibly challenging (Matthew Hudson, Interview, 2015). It meant that the IT department was trying to make sure all data, even data that did not have government regulations as strong as HIPAA regulations, was heavily guarded in a similar manner to medical records. Lawrence stated that:

> Well, how much can we really secure this environment anyway? I think the IT community here at the University has done a really good job. And I'm not 100 percent up-to-date on where we are, but coming up with new standards, not just new rules of what to do, but a way of looking at and trying to right-size the risk assessments, right-size the approaches we might take in dealing with things. (Kyle Lawrence, Interview, 2015, 06:15)

For example, instead of assuming that all data must be protected, he believes institutions should examine the different types of data and assign the correct level of security for that specific type of data. In dealing with his college's data needs, Lawrence stated:

> We're going through a process to say, "Okay, generally, the college is at a low-level of data needs." And then by moving up the line, maybe certain departments move up that line and then maybe certain individuals go higher up and we kind of right-size the security. I think, in our past we took the reverse approach. This was a good five, six, seven years ago where we just kind of assumed everything is a part of the data, and we'd protect it unless we knew otherwise. (Kyle Lawrence, Interview, 2015, 07:00)

This directly correlates with the data classification standard launched by the institution. This standard leads to an ability for the institution to focus more resources on securing the data that presents the most risk to the institution, instead of worrying about all of the data which is often too large of a job to manage successfully. Lawrence recognized that there are always security risks, but the institution is more risk-accepting right now which reflects the reality of today's work environment. Lawrence stated:

> We're moving from a risk-adverse culture to more of a right-sizing it, a more risk accepting, which I think is good and I think is more flexible for the faculty or TAs or everybody who has such a mixture. (Kyle Lawrence, Interview, 2015, 8:15)

There is always risk, but it's about focusing on the biggest risks and addressing those.

Hudson agreed that focusing on all data as a risk was unsustainable, and that creating more classifications and building some levels inside their security controls made the institution able to "right-size" the type of security that was appropriate for each type of data (Matthew Hudson, Interview, 2015). This allowed them to dedicate more resources towards the data that needed the most protection, like HIPAA data, and dedicate less resources towards data that presented a lower risk. The community approach was used when developing this policy, meaning that campus was heavily involved, and Hudson indicated that was critical to the successful adoption, implementation, and awareness of this policy (Matthew Hudson, Interview, 2015).

The institution utilizes a central cloud-based e-mail solution for all areas of the institution. However, Lawrence indicated that there are certain services, such as the health center, that have to adhere to stricter privacy standards due to HIPAA. Though they are using the cloud e-mail as well, they have their own separate implementation of it

in order to ensure they follow stricter guidelines. Referring to the computers that access HIPAA, Lawrence stated that:

> That domain has more restrictions on it, versus the general everybody domain that everybody else is in: students, staff, faculty of the other colleges. (Kyle Lawrence, Interview, 2015, 10:38)

All three interview subjects agreed that these areas have a need to deviate from the central approach slightly in order to ensure that their data are properly protected per HIPAA regulations. The cloud-based e-mail solution in the healthcare area forces passcode, encryption, and other policies onto any mobile devices that are used there, while the cloud-based e-mail for the rest of campus does not enforce these same restrictive policies. Hudson states that universities overall are an "extremely open type of culture and environment" (Matthew Hudson, Interview, 2015) and their institution has a similar culture. The fact that they were able to implement a light mobile device management solution through the cloud-based e-mail solution is a pretty big win in an area that is traditionally so open, according to Hudson (Matthew Hudson, Interview, 2015).

Lawrence indicated that it can be complex to navigate between the two environments and ensure that people can communicate appropriately across the two environments. For example, a faculty member in the more restricted area may want to collaborate with another faculty member outside of the restricted area. The interview subjects stated that it is important for higher education institutions to balance access and security in order to ensure that employees can still collaborate and conduct the business

that they need to in order to reach their educational goals (Kyle Lawrence, Interview, 2015, 11:34).

Hudson states that security architecture, which refers to the designing IT systems in a secure manner, and risk management are two critical pieces that are being focused on in order to help move the institution to a more secure framework (Matthew Hudson, Interview, 2015). The development and inclusion of a risk management program is a critical focus for the IT security department at this institution. Hudson discussed how important risk management is to the entire institution but particularly to leaders. In order to make informed decisions, leaders need to know the strengths and weaknesses of the institution (Matthew Hudson, Interview, 2015). They need to know what risks are the most critical to address, and often this is done by doing a gap analysis to determine where areas of growth may lie. Hudson indicated that the institution has not fully adopted any specific security architecture or framework model, such as NIST or the SANS Top 20 Security Controls, but rather seeks to address the institution's unique needs (Matthew Hudson, Interview, 2015). Regardless of which model or standard is utilized as a guide, it is impossible to meet every control but according to Hudson, it is important to evaluate the approach intentionally and determine which risks need to be addressed (Matthew Hudson, Interview, 2015). This is where a personalized gap analysis becomes incredibly critical to an institution's successful risk management or security program.

The mobile device landscape at an institution of this size is incredibly diverse. Logs are pulled from e-mail, wireless network, and web data occasionally to assist in determining what types of devices are being utilized on campus and by visitors to the institution, but all interview subjects indicated that the variety of devices and the ever-

changing nature of mobile devices makes it difficult to know what faculty, staff, and students are using to connect to campus resources. When asked about personally-owned versus University-owned mobile devices, Lawrence stated:

> It's a total mixture. There's no clear line who owns what anymore. There are things that are specifically purchased by University funds, and we know that those are University-owned. There are things that are purchased by individuals, and we know that those are personally-owned, but the usage of those is a total mix. You'll see iPads or tablets, and you will have no idea who bought them. Some people buy them with their own personal money; some people had money in their budget and buy it, but the usage is exactly the same. (Kyle Lawrence, Interview, 2015, 03:45)

Lawrence further stated that he does not foresee this becoming any clearer in the future and that it will only continue to grow in diversification. He stated that:

> We attempted, in years past, to be very rigid and specific about "it's University-owned, and this is what we can support" or "it's your personal device, and we can't touch it." All that stuff needs to disappear because it doesn't match the reality of what people's situations are anymore. (Kyle Lawrence, Interview, 2015, 04:20)

The institution is being faced with an ever-increasing and ever-changing body of devices, and interviewees were clear that the old ways of securing data will not be successful. "We need to change the options to reflect a multi-device reality" (Kyle Lawrence, Interview, 2015, 05:50). Interview subjects seem to agree that it is nearly impossible to control the constant inflow of devices and that it is necessary to stop trying to control the

devices and instead devote resources towards protecting the data assets regardless of where or how they are being accessed.

Brooks stated:

> I think we've done well protecting the data, not the devices. That's kind of made the devices a little bit… I mean, they are an incoming vector, but they are just another one. There are some unique aspects to it, but as long as we are protecting the data that actually has the most risk, I worry less about the endpoint. (Duncan Brooks, Interview, 2015, 13:48)

Brooks further explained that the data are where the most risk lies, and it is less critical to protect the hardware and more critical to ensure that the data assets themselves are protected. Brooks jokingly stated:

> There's not going to be an article in the [local newspaper] saying that "The University lost one cell phone." If you risk just a cell phone, I can live with that. However, if the story says "the University lost 5,000 patient records," that would be bad. (Duncan Brooks, Interview, 2015, 14:31)

Lawrence indicates that there is an inventory of mobile devices. However, looking forward, he is advocating that it is becoming less important to manage the devices themselves. Lawrence stated:

> I have actually been advocating for not trying to keep track of it, manage the money but not managing the devices anymore. It would reduce a lot of workload for trying to keep track of it. Getting a lot of pushback on that for good reason. But as far as mobile devices, it's too easy to just go pick them up. For University funds, go out to the bookstore and you're done. There's no checks on that, even to

> make sure they get an inventory sticker on it. So trying to manage and keep track of that is very difficult. (Kyle Lawrence, Interview, 2015, 15:41)

Lawrence's idea is that moving forward, they would sit down with each faculty member, consult on their individual needs and help guide them in the right choices that assist in helping the faculty member reach their educational goals while still complying with the necessary security requirements to protect institutional data. Lawrence stated:

> My idea would be that we're sitting down with every faculty member and talk to them about their needs, and we should have some more of an individual plan for them. How can we help you? How can we identify what your needs are? And, at that point, kind of gather information about what they're using. That's what I would like to do at some point. (Kyle Lawrence, Interview, 2015, 16:35)

Lawrence indicated that policy alone won't fix security issues and that institutions need to help people understand and be more aware of security risks and the solutions available to safely store and use data. Lawrence stated:

> The technologies are also driving the change because they're becoming more flexible, and now your device is just a dumb terminal, a window to some content stored elsewhere. Obviously, we can't guarantee that. Obviously, a lot of people under very old practices and still maintain their spreadsheets or they're storing data that they shouldn't be in the wrong places. And I don't think policies necessarily will fix that. It's more, as technologies change, help people better adapt to how to use the technology better and to be more informed. Your device is just a dumb terminal, a window to content that is stored elsewhere. (Kyle Lawrence, Interview, 2015, 09:00)

For Lawrence, the key is the intersection between security and being able to allow the faculty and staff to complete the work. Lawrence states:

> I think I would like to educate the whole community on where do I store my data? What device do I use? Not always as a way to secure, although that's the key issue for some people. But where it [technology] works, it's convenient. It helps make sure that I'm ready to teach tomorrow. I want people to be more in charge and more aware about how to deal with such a changing environment. They want to work anywhere on any device at any time and be flexible. And they can survive day-to-day issues. I want people to have that comfort and skill set. That's going to come from process and training. But everyone's situation is going to be different. It's going to come from catching them at the right time with the right need to update them on what they can do. Security should be part of that, but I want them to own it in a way that they take responsibility and say, "This data is important to me and I now feel comfortable and know how to make the right choices on where to put it." (Kyle Lawrence, Interview, 2015, 18:12)

Interviews indicated that some faculty and staff appear to be most concerned about ownership and privacy of their information and research, as well as being able to complete their work. Lawrence indicates that faculty and staff are more concerned about who owns their data when they put it in the cloud and less focused on the devices they are using. Faculty want to be certain that a company such as Google does not suddenly have access to their data once they have put that content online. Lawrence stated:

> I would say that I get the sense that they're more worried about mobile device, in certain issues, than they would've been in the past. I think they are maybe more

> concerned in general about things they hear on the news, techie stuff. There's probably a significant population that's probably worried about Google and them having access to our content and the broader privacy issues from government access and who owns the data. I think that the content is more of their concern than it is about my device is not as secure as I want it to be. Even in the past, it was never that they wanted more security. It was just all the security was just annoying to them. (Kyle Lawrence, Interview, 2015, 22:54)

Brooks stated that he doesn't think the average faculty and staff think a great deal about security. Of faculty and staff perceptions of mobile devices, he explained:

> I don't think they think about it too much. The only reason that I'm saying that is because usually we have to explain why they have to do something a little bit different if they do use legal and private data on their mobile device. Like they're not reading it and then going, "Oh yeah, that makes total sense" all the time. But I think they have generally gotten it. We have pretty good training. It's not fancy, but it's just some online courses we make everyone go through. And they have to work with that kind of data to cover some of those topics. That does a pretty good job of just helping them understand what our concerns are and what their role in protecting the University is. (Duncan Brooks, Interview, 2015, 15:35)

Brooks further stated that:

> The people are the weakest link in my opinion, more often than not, with social engineering stuff and bad data management practices that are really hard to defend against. (Duncan Brooks, Interview, 2015, 16:21)

All interview subjects at this institution agreed that the faculty and staff are most concerned with being able to successfully complete their work and that IT should focus on ensuring that the security measures employed do not inhibit the work of the institution. However, all agreed that is a difficult balance to maintain because of the diversity of the work being done at the institution and the changing nature of security.

Future plans and trends.

The following interview questions were asked by the researcher in order to determine the interview subject's perspective on the direction of mobile device security, both at this specific institution and in the industry at large:

- What trends do you see coming in the future regarding mobile devices and/or security?
- What do you think your institution does regarding the security of mobile devices that needs improvement?
- What resources, processes, policies, et cetera do you wish your institution had to assist with the security of mobile devices?

When asked about trends that were coming, Hudson discussed how, years ago, mobile devices were supposed to be the next attack vector, yet that is still is not happening despite predictions that it would (Matthew Hudson, Interview, 2015). Brooks agreed with the assessment that devices today do not appear to be targeted for malware quite yet. He stated that "we haven't had lots of malware issues or anything in that space" (Duncan Brooks, Interview, 2015, 12:59). Hudson thinks it is still possible that it is coming in the future, but as people move away from storing mass amounts of data on the device and access that data in the cloud instead, it makes the device less of a target

(Matthew Hudson, Interview, 2015). Years ago, Hudson stated that many IT departments were working hard to build rigid mobile device management systems that locked down the devices, and in some cases prevented personal devices from connecting at all, with the goal of protecting the institution's data (Matthew Hudson, Interview, 2015). Today, Hudson observes departments backing away from that because it disrupts the individual from being able to do their job. Today, Hudson stated that IT departments are trying to find the right balance between access and security, and that work will need to continue in the future as technology developments continue to evolve and change (Michael Hudson, Interview, 2015).

Other trends the interviewees highlighted as growth areas involve accessing things anywhere, anytime, including the idea of virtualizing software so it can be accessed no matter where you are without installing anything on your device, further emphasizing the decreasing importance of the device itself. Brooks agreed that trends continue to show an ever-changing body of mobile devices entering the institution, stating that:

> We've been living in this half University-owned, half personally-owned device world for a while, and the growth of the mobile device is just an expansion of that. The wireless network experiences issues keeping up because people now have three devices connected to the network now; their phone, their iPad, and their laptop, but that's not really so much a security issue as a capacity issue. (Duncan Brooks, Interview, 2015, 10:57)

Brooks further explained that while this also puts increased pressure on staffing to support those devices, at the same time, "It's gotten easier, though, because our wireless

network has gotten better and also because the devices connect easier than they used to" (Duncan Brooks, Interview, 2015, 11:41). As they have continued increased pressure to provide wireless capabilities and support, they similarly have increased pressure to ensure their data are secure no matter which of the three devices their end user happens to be using to access institutional data. Because this continues to grow as more devices are added, the institution is recognizing that need to focus on the data in the future because it is nearly impossible to ensure that all the devices are secure.

When asked about resources needed in the future to assist with the mission of mobile device security, Hudson stated that rather than investing more resources internally in the security team at central IT, he would prefer resources to instill security into the mindset of IT professionals across the entire institution, both through educating them and helping them care about security on a regular basis (Matthew Hudson, Interview, 2015). All interview subjects agreed that mobile device security cannot be limited to the purview of just the security IT team, but involves all aspects of the organization.

Communication and training.

Though no specific interview question was focused on communication or training, this arose as a theme from each interview. The framework of IT security at this institution appears well established and centrally-managed, despite the fact that IT services themselves are distributed, and the communications framework to accompany that structure is equally well established. Hudson indicated that funding for security initiatives is well-understood at this organization and something that is given priority and discussed broadly (Matthew Hudson, Interview, 2015). Hudson indicated that a centralized focus on IT is critical to the success of their initiatives because having that central, over-arching

responsibility for IT security is imperative towards seeing the main risks and mitigating those risks. However, he also stated that while a central focus is important, it is equally important that everyone at the institution be aware of and involved in security issues to some degree. This “community approach” was mentioned by Hudson as the most important aspect of building a strong security program. He further explained that it helps to get buy-in from the institution if stakeholders are involved early on in the process of making security decisions and policy for the institution (Matthew Hudson, Interview, 2015). Gathering feedback, listening to the community, and ensuring that people have a voice in committees and task forces can dramatically increase buy-in once security initiatives are launched.

Hudson stated that security awareness training is handled primarily by the IT security department, but it is also a partnership where all IT staff are responsible for some amount of security awareness (Matthew Hudson, Interview, 2015). When introducing new policies and new trainings, Hudson stated that he was given an excellent piece of advice a long time ago that said, “If you think you’ve communicated enough, double it, and then double it again” (Matthew Hudson, Interview, 2015). It is clear from the interview subjects’ comments that communicating with faculty, staff, and students is a fundamental piece of every step of the security process, from creation to implementation to support.

New employees to the institution complete security training upon entering the organization. Lawrence states that there are mobile device security policies, such as passcode requirements, that apply to those that work within specialized areas, such as the health center, and some training for folks who have those roles (Kyle Lawrence,

Interview, 2015, 09:58). There are also training modules available on data security, but these are not specific to mobile devices in particular. Overall, the communications and training plans around mobile device security appear to be fairly robust in nature.

Case Study #3 – Institution C

Introduction.

Institution C is a large undergraduate and graduate degree-granting institution in the central United States, similar in size to Institution B. It serves over 30,000 students and over 15,000 employees (University web site). There are many different campus locations, and instruction happens using a variety of methods including face-to-face, online, and distance learning. Faculty have an extremely strong voice in this institution's governance. Four interview subjects from this institution included Michael Gregory, Kevin Johnson, Dylan Weston, and Alex Bennett, who all work in various IT roles throughout the University; three within the central IT department and one in a distributed IT department.

Environment and staffing.

The following questions were asked by the researcher to assist in creating a picture of the environment at this institution:

- Please describe the role you take in working with mobile devices and/or security at your institution.
- What do you think the perception is of the security of mobile devices by the faculty and staff?
- What do you think your institution does well regarding the security of mobile devices?

The IT staffing and support on this campus is a mix of centralized and decentralized structures, with strong emphasis on maintaining decentralization in order to address the specialized needs of each area. Because of the highly decentralized nature of the IT support structure, it makes counting IT staffing levels nearly impossible. Not only are there many distributed help desks, but there are also individual IT staff housed all over the institution (University web site). This institution does have a designated security department with a new CISO position leading it.

The administration of security on this campus is extremely decentralized, with some IT security work being done by central IT and some being distributed across campus. Each department has their own IT people, and interviews suggest that there is little central governance of those distributed departments. For example, though there is one main firewall for campus, there are many individuals across campus with rights to adjust the firewall settings for their unique distributed areas. Gregory stated:

> It is just simply this is the way we prefer to do business is having it open. And, you know, I've been in higher education long enough to know that it is all about making sure that you can get the information you need to get. You know, we do our fair share of black-holing, white-listing, et cetera. But, in a mobile environment, it's all about letting them have access. And we have plenty of bandwidth to go around, so it's not a constraint issue. It's simply just opening up the attack vectors by increasing the surface because of so many mobile devices. (Michael Gregory, Interview, 2015, 17:10)

Mobile devices play a major role in this institution. Gregory stated:

> When you talk about the world of mobility on campus, you're talking about a heavily student population and a heavily researcher population. And then, of course, all of the staff that works here, they enjoy having the, you know, the Dell Latitude laptops, and their various Mac and other platforms. We are a laptop society here. (Michael Gregory, Interview, 2015, 06:25)

Gregory acknowledges that tablets and mobile devices are becoming a growing focus as well. When asked to explain a bit more about why mobile devices are so integral in their institution, Gregory continued:

> I think it's just an understanding that, in this type of environment, you have to be mobile. And there is a little bit of doctrine and strategy behind it. The cost of laptops has come down, so we can do that. We have a very robust infrastructure here, so putting on wireless devices is something that we've got in our strategy. We are doing it actually right now and just the need to be mobile-friendly in the commons. In the buildings, we don't have all the money in the world to run wired environments, so we are going to run as much through wireless as we can. (Michael Gregory, Interview, 2015, 07:20)

Johnson stated that:

> I do know that at any given time we have, I think, in the neighborhood of 40,000 endpoints accessing our network. I would state that the vast majority of those are mobile devices. (Kevin Johnson, Interview, 2015. 03:47).

In terms of the mobile device landscape, this institution has a vast array of devices currently being utilized. Some data can be collected via the network, e-mail, and web site traffic, but this is not something being examined regularly or in great detail today. When

asked if they collect data about mobile device usage, Johnson stated that “the help desk does not” (Kevin Johnson, Interview, 2015, 08:56). This institution has a strong wireless footprint on campus (Michael Gregory, Interview, 2015, 03:49). Gregory explains that “we have certain environments that are multifactor” meaning that they are using multifactor authentication and that “we would like to go further” in the future. (Michael Gregory, Interview, 2015, 14:30)

There are several help desks across the institution. According to Johnson, one of the largest help desks at the institution supports both personally-owned and University-owned devices, and they “do not treat those devices any differently” upon setup (Kevin Johnson, Interview, 2015, 09:58).

The mobile device landscape at this institution is very diverse. Interview subjects surmised that most smartphone devices are personally-owned because the institution does not buy a great deal of smartphones. However, Weston stated that University-owned tablets are increasing in popularity. Weston stated that:

> Tablets have been picking up a little bit more in popularity. People have been wanting them, and departments have been buying them. They're a little easier to support in general because they're a little closer to a laptop. But at this point, we're still in the phase of we'll try, but we can't guarantee anything. (Dylan Weston, Interview, 2015, 06:39).

University-owned assets are tracked in inventory, and that includes basic information about the type of device, but little else. Overall, interview subjects agreed that it was difficult to get a clear picture on the mobile device landscape because of the variety and quick rate of change.

Johnson indicated that an area that this institution excels today is in managing devices that have gone missing. He stated:

> I think we have a very good process for managing devices that may have gone missing, in terms of having that central point of contact for that. We work very closely with our police department so if someone happens to call them about a missing device, the police will do whatever reports they deem necessary, and they will coach the person to contact us to get the security response team up to speed on whatever might be going on. I think we work, given the decentralized nature of our campus, I think we work very well with the security group to make sure that we are actively involved in helping develop that process, tweak that process for future use. And we work them, actively, throughout the year, helping them to test that process to make sure that it's working. (Kevin Johnson, Interview, 2015, 15:43)

Johnson also indicated that he believed faculty overall were quite security conscious. He stated:

> I think, if I were to look across the faculty that we have here, I think that they are actually very security conscious, particularly as it pertains to their individual domains of research. (Kevin Johnson, Interview, 2015, 18:55)

When asked about the perception of faculty and staff around the topic of mobile device security, Bennett stated:

> You know, it is mixed. They want the absolute best performance and easy access and easy use. And they want it to be as secure as possible at the same time, and the challenge is that there is usually tradeoffs associated with that. They basically,

> well, most of the staff just want the network to be easy, fast accessibility to their data, and the assumption is that the security is taken care of. (Alex Bennett, Interview, 2015, 17:08)

Governance and systems.

The following interview questions were asked by the researcher to determine what technical systems, policies, and other frameworks for decision-making were in place at this institution:

- What policies and procedures does your institution have regarding the topic of mobile devices and security of those devices?
- What types of systems do you use to manage mobile devices (example: Mobile Device Management solution (MDM) or something similar)?
- What information does your institution collect about mobile devices and usage by faculty, staff, and/or students?

Governance at this institution seems well-established, despite the decentralized nature of the IT environment.

Gregory stated:

> We have a pretty robust IT policy group here that is organized around the campus. We do distributed governance and shared governance, and by that I mean we have governance bodies that are all over campus at all levels and really focused on the student experience and support of faculty doing the things that they need to do to deliver instruction. But we also have a very robust research environment here on campus. (Michael Gregory, Interview, 2015, 04:25)

In order to properly support that research, Gregory stated that these governance bodies ensure that all policies are reviewed and that they do not inhibit the research that is so critical. However, obtaining resources for the security of mobile devices is often still a problem without a solution.

Gregory stated that:

> A lot of the research work is sometimes done on an IT shoestring. That's the last thing they are worried about. They are more worried about getting the research done and accomplished and all that. We aren't going to have an awful lot of cabled infrastructure for doing the research. It's all going to be on laptops and mobile devices. This causes problems sometimes if research is done which requires access to restricted data, PHI and other data that is covered under HIPAA and HITECH, so we do have to be very careful about how we approach that. (Michael Gregory, Interview, 2015, 05:30)

In light of the importance of research at this institution, Gregory stated that as needs frequently change around mobile devices and security, Gregory stated:

> We [the institution] are going to evolve our policy. I'll throw my "new kid" card on the table here. We are going to be a lot more agile in policy development. (Michael Gregory, Interview, 2015, 08:40)

This is in response to faculty's needs around technology and research, which sometimes change frequently as there are new advancements in their research and the capabilities of mobile devices.

Gregory stated that:

> We are all about the faculty and having them have the tools they need. Sometimes the governance is a little bit slow to react and get to the point of being able to do that. And, of course, you've got all the IT guys that are full of great ideas; and we [IT staff] want to do the bigger, better, faster, cheaper kind of planning. But that's not what the faculty wants, so we have to spend our time and our shared governance bodies to listen carefully to what the faculty are saying and provide them with what they need. (Michael Gregory, Interview, 2015, 09:05)

Gregory feels that the institution needs to become more agile to adapt more quickly to these changing needs in the future, and they are working on doing that with a keen eye on how to include the faculty and staff in those decisions.

Faculty are asking for increased wireless and mobility in order to perform their research and teach their courses, and Gregory stated:

> So there are faculty that are screaming wireless. There are faculty that are screaming mobility. And we're to the point where we're able to respond to them appropriately. (Michael Gregory, Interview, 2015, 09:46)

Gregory stated that the faculty are aware of security, but "they [faculty] are wanting security, but they don't want security to stifle research, and they don't want security to become the main picture" (Michael Gregory, Interview, 2015, 10:28) Gregory further explained, stating that faculty "want as much security as is necessary to keep education running but not more security that would be intrusive and halt what they are doing in the classroom" (Michael Gregory, Interview, 2015, 10:42).

Interview subjects agreed that the vast majority of users do not need super intense security controls on their mobile devices. Most faculty and staff needs are fairly basic. He estimates that:

> I would say it would be in the high 90s of systems that connect that don't need any security features whatsoever. They just need access to the Internet to get to whatever site they get their data. (Michael Gregory, Interview, 2015, 12:18)

When discussing whether there is a need for a more robust MDM solution, Gregory stated:

> The need for something like a robust MDM, and I'm thinking like a MaaS360 or the latest product from Good Technology, I don't know if it's justifiable other than a warm fuzzy feeling that you've done the right thing. If we are going to get penetrated and if somebody is going to start exfiltrating data, it's going to happen whether on wireless or VPN. Either way, they are going to bust it. They're going to get in, and life is going to be rough for a few weeks. If I were to do anything, it would be to at least register devices. (Michael Gregory, Interview, 2015, 12:35)

Gregory further explains that this would help them in finding and identifying rogue devices. "Right now, everybody is rogue. And you have to wait for a leak to happen before you are able to investigate appropriately" (Michael Gregory, Interview, 2015, 14:00). Registering devices would allow the institution to allow access for all registered devices and block out devices that were not registered, thereby securing the environment from an attacker. Gregory stated:

> If I could find an elegant way to register devices and then have an MDM solution that would allow me to at least throttle and be aware, I would probably be in a

> much better position to make stronger recommendations on services and such. But we have conditioned our enterprise appropriately so that it's not a free ride but it's not the most secure it could be. (Michael Gregory, Interview, 2015, 17:57)

All of the interview subjects discussed the importance of balance between access and security. More security can sometimes lead to less access, and the interview subjects felt that would greatly inhibit the mission of their institution to allow research, exploration, and innovation. Gregory stated that "in a mobile environment, it's all about letting them have access" so that they can complete the work that they need to do (Michael Gregory, Interview, 2015, 17:30). Gregory believes institutions should be asking the questions to get a proper use case in order to determine the right levels of security. Gregory stated:

> If I have a University device with a proper use case, then part of that proper use case is going to be "What security does it need? Where's it going? What's it getting when it gets there? What's it doing with the data? Am I encrypting the rest on the device?" (Michael Gregory, Interview, 2015, 30:38)

Gregory stated that it's important to consider these items when determining and aligning the right level of security needed for mobile devices.

The return on investment for security needs to be a critical concern for institutions, according to Gregory. Gregory stated:

> I've been taught for many, many years in the information security business that you never impose a countermeasure where the cost of that countermeasure is going to exceed the value of the resource. (Michael Gregory, Interview, 2015, 39:35)

This means that if a security measure or policy is going to give you a certain benefit, but it is extremely detrimental to the environment, faculty research, or the student's learning experience, it simply may not be worth it. Gregory stated:

> When I'm negotiating for a future mobile device management solution, I have to be able to have that ROI that tells me that if that solution is costing me more than "X" dollars per device, then I'm not helping. (Michael Gregory, Interview, 2015, 40:37)

Gregory stated that "It's about how much [security] you need to do the job of education" (Michael Gregory, Interview, 2015, 28:21).

Overall, processes at this institution are quite well-established. There is a very well-defined security procedure for incidents such as lost or stolen devices, and these processes are coordinated through a cooperation of the help desk area and the security team. Johnson stated that:

> We actually have a security response methodology that we follow from our help desk that involves us contacting immediately the security department, and the first thing that they do is speak with the end user to determine any risk for data that may be on that device. (Kevin Johnson, Interview, 2015, 11:00)

Though there is no specific mobile device management software used at this institution, the institution will have a light version of those capabilities soon. There are a variety of e-mail systems on campus today, but the institution is moving towards one centralized cloud-based e-mail system for the entire institution. This system can force a passcode on mobile devices upon the first connection to the institution's e-mail, acting as a sort of mobile device management system.

While there is no single MDM system at this institution, the institution is making a commitment to move towards a central solution for e-mail and other services, which provides a few of the functions of an MDM, is a step in the right direction, according to interview subjects. For example, this solution does provide remote wipe capabilities, which can remotely wipe all of the data off of a mobile device as soon as it has connected to e-mail, just with a few clicks of a button. This solution can enforce some policies such as requiring a passcode and encryption. Interviews indicated that some of these policies are not currently activated at this institution but there is room to add them in later if the institution chooses. The advisory groups have had discussion about the remote wipe capabilities of this e-mail solution, and there were mixed feelings about this feature. While this does allow for increased security and some added peace of mind if someone's device is stolen, it also makes many faculty and staff fearful of the institution's power over their device.

Passcodes are recommended by IT professionals, though not required. Weston stated:

> Passwords are a big one. Password protect it whenever possible. For phones, for example, a lot of them have a screen locking feature. I typically advise people to actually use them because if you lose your phone and you don't have that set up, then whoever picks it up is you. (Dylan Weston, Interview, 2015, 13:02)

He continued, "of course, if you do have one, they just picked up an expensive paperweight" (Dylan Weston, Interview, 2015, 13:39). Acceptance of a passcode varies from user to user, according to Weston. Weston stated that without a larger passcode

policy, those recommendations aren't always successful. In talking about acceptance of passcodes on mobile devices, Weston stated that:

> It's sort of varied. It's varied from user to user. Some of them are all about security. They just eat up everything you say, and they're happy to put passwords on everything and just are very security-conscious people. Others, they're not really concerned. All they really want to do is do research, and they want that to be as easy as possible. For them, they don't want to have to type a password every time they open up their e-mail. They just want it to open. (Dylan Weston, Interview, 2015, 13:54)

Though IT at this institution is extremely decentralized, the many cross-University advisory groups help inform and guide the institution's strategic direction for technology. Weston stated that there is "an advisory group, basically with voting members from different departments off-campus, and they all advise the main CIO office" (Dylan Weston, Interview, 2015, 01:47). Weston further explained:

> Membership is open. It's not limited to anyone in particular, but there is only a select set of them that are considered voting members. But, again, they don't really make the policy. They just advise the CIO and his group, and they actually make the policies. (Dylan Weston, Interview, 2015, 02:41).

Many attendees on the advisory group for technology security also belong to other advisory groups as well, ensuring that there is continuity among the information shared. Often topics, initiatives, or policies that are discussed are brought to multiple advisory groups to ensure that more perspectives are included. Those interviewed stated that it is often difficult to determine the appropriate level at which decisions should be made with

such a varied IT structure but that, overall, the advisory groups assist a great deal in making the campus community feel heard, which in turn assists in their buy-in as ideas become policy or projects. All subjects interviewed stated that the faculty are heavily involved in the institution and are a very strong voice in guiding what happens there.

In regard to policy, many of those interviewed stated that BYOD, or non-University-owned devices, can create a grey area. According to Weston, there is a campus-wide security initiative underway currently to move all University-owned computers to a base level of security, but this does not impact mobile devices nor personally-owned devices at this time. Weston stated:

> They've been meeting for some time now trying to work out some policies, basically how to handle some of this stuff. And the last I heard, they met in March and advised the CIO on what their official recommendations were. Since then, I haven't heard anything, so we're kind of at the grey area right now as to whether we support/not support what's required on these devices. And it's really done on a case-by-case basis and a department-by-department basis. (Dylan Weston, Interview, 2015, 04:08)

Because these devices are new and because the technology is changing so rapidly, there appears to be a gap right now in that the IT department knows they need to support these devices but they are not quite sure how to do that with limited resources and so many kinds of devices. The IT support professionals that were interviewed stated that they do the best they can to help their customers do what they need with their devices when it comes to University-related functions such as research, but that they cannot guarantee they can make everything work for their users. Similarly, they aren’t sure how

to properly secure all the different types of devices and all the different types of data end users are trying to access. Without all of this information, interview subjects mentioned it can be difficult to communicate clear, understandable policies and procedures when there is so much still unknown. Essentially, Weston stated that support of personally-owned mobile devices is a best-effort level of service because of all of these variances and a lack of dedicated resources specifically for supporting mobile devices.

Weston indicated that users themselves and their habits are still one of the biggest risks to security. He stated:

> We try our best to educate the users and get them thinking about security because at the end of the day, it doesn't matter what security measures you have on your phone if the user themselves doesn't want to use it or doesn't know how to effectively use it. And we don't have any massive training programs in place, but whenever someone brings us a phone or a tablet, we do try and instill that idea that security is an important thing. (Dylan Weston, Interview, 2015, 14:58).

Weston stated that each time a faculty or staff person comes in with a mobile device, they try to talk about security best practices. Speaking of supporting mobile devices, Weston stated that:

> It’s a difficult problem. There’s a lot of different types of devices out there, and providing support for it is not easy. Every different model, every different operating system that is on them is going to have different applications and different security measures, different security holes. It’s hard to plan for all of that variability. (Dylan Weston, Interview, 2015, 17:25)

Staffing, training, and resources are all needed in the future to improve security, according to Weston, and he stated, “it is a staffing issue; it's also a training issue. We just don't have the resources to really do that at this point” (Dylan Weston, Interview, 2015, 18:11)

Future plans and trends.

The following interview questions were asked by the researcher in order to determine the interview subject’s perspective on the direction of mobile device security, both at this specific institution and in the industry at large:

- What trends do you see coming in the future regarding mobile devices and/or security?
- What do you think your institution does regarding the security of mobile devices that needs improvement?
- What resources, processes, policies, et cetera do you wish your institution had to assist with the security of mobile devices?

When asked what types of resources may be needed in the future, the answers varied, which is indicative of the different roles of the people that were interviewed. Because they all see a different piece of the security puzzle, they all saw unique needs that pertained to their areas. From the support side, interview subjects indicated that increased training and support would be beneficial to help them improve the support they provide to their customers. From the infrastructure side of the shop, increased technical capabilities such as multifactor authentication and improved encryption were cited as potential growth areas in the future. All interview subjects agreed that policy is a major

area that needs to be focused on in the future, and letting the campus community have a voice in that policy creation is critical.

When asked about the biggest need for their institution in the future, Bennett stated that the biggest challenge has always been securing the devices themselves. Bennett stated:

> Obviously, the challenge until recently for us has been in trying to simply create an environment where we could secure the device itself and having enough profiles that worked in that environment. I think trying to move some of that capability off of the device and potentially into the network or into the cloud even, to some aspect where we could consume the resources necessary to collect and manage more of that information. (Alex Bennett, Interview, 2015, 12:35).

He further explains that the device needs to be less of the focus, and the focus should be on securing the network and data regardless of what device is being utilized. Bennett stated:

> The devices will continue to change, and the other thing is because of the diversity. There's not like an enterprise architecture where you can close down, require people to use specific devices or they don't get access to the network. It's an open environment, and you basically have to move the security more into the network rather than on the device itself from our perspective. (Alex Bennett, Interview, 2015, 13:56)

Bennett stated that even with the robust mobile device policy that exists today, that policy could still use a bit of improvement. When asked about what could be improved, Bennett stated:

> Probably just establishing policy related to the security aspects of the network. That's something that, in a very autonomous environment that exists in the network, that can be somewhat difficult to agree upon and then to implement. (Alex Bennett, Interview, 2015, 16:16)

Though it can be difficult to agree upon and implement, it is still needed to help keep faculty, staff, and students aligned on security regulations. There are cross-campus groups that work together to discuss these policies but that can take time, and the role of the decision-maker is not always clear. Despite the extra time this takes and the difficulty in determining who has the ultimate authority to approve the policies discussed, Bennett stated that “the more that that [policy] can be discussed and that there’s an opportunity for the wider campus to participate in the conversation, the more successful the outcome can be” (Alex Bennett, Interview, 2015, 20:11).

In discussing the future of mobile device support at this institution, Johnson stated:

> I really don’t see any change in the support that we provide for those devices. I think we have an overly flexible environment where we don’t manage devices, but it seems to work here. Particularly because if you look at our faculty, in particular, we are a highly decentralized University, and the faculty and students pretty much get to choose whatever devices they want to use. And our IT environment on campus is highly decentralized, and I see some minimal consolidation of that in the next year or two due to budget issues. However, in terms of mobile device management, I don’t see us consolidating on any mobile

> device management platforms or increasing requirements for the use of mobile devices in the near-term future. (Kevin Johnson, Interview, 2015, 13:47)

Johnson feels that the flexibility of their mobile device support strongly compliments the needs of their institution, allowing their faculty to do the work they need to do, and this is a trend that he is seeing all over the field of higher education. Despite the fact that Johnson does not envision a large-scale mobile device management system being adopted in the near future, he stated:

> It would be nice to have a more consolidated environment. I think the distributed environment that we have works well, but you really can never be sure what's going on with those mobile devices without that MDM in place. I think it would be helpful for us to find a solution that might work for our organization that allows us a little bit more control than what we have over those devices. (Kevin Johnson, Interview, 2015, 17:15).

When looking towards the future, Weston stated that:

> Tablets and smartphones are getting more and more widespread. They're also getting more powerful. So, previously, something like a tablet, you're not going to be able to do a whole lot on it. But as the technology improves, as more people buy it, Microsoft pours more money into it and Apple and other companies, more and more people are going to want to use them. And when they become that widespread, it's going to be something that has to be dealt with. Right now, it's still not widespread enough to devote all this effort, or too much effort, to actually get these policies in place and actually support these devices. But, it's going to be

> something I think is unavoidable in the next year or two. (Dylan Weston, Interview, 2015, 11:43).

Gregory discussed the important trend of credential-based authentication and multifactor or one-time passwords. Gregory stated:

> I came from industry. And the folks that we worked with and the folks that we gave our advice to, we were very heavy on getting that MDM in there and using it appropriately. I mean, it's not enough just to plug it in and say "it's there." It's, what are the rules you're setting up on there? What are the authentication mechanisms you're putting in there? It can't just be username/password. You've got to go multifactor; or you've got to go one-time use password like RSA or something like that in order to really call yourselves secure enough to be in the business. (Michael Gregory, Interview, 2015, 24:29)

Interviews indicated that one item trending in the future is two-factor authentication, also called multifactor authentication. Bennett stated:

> The challenge is, how secure do we need to make the wireless network? We have to begin to make it more and more secure because in the past, those type of applications were typically confined to the wired network, and that increased the security of aspects of the network. Through the wireless, you really don't know who is tied in and listening, and I think that multifactor authentication, higher levels of encryption, and the continued increase in performance are things that are going to be desirable in the future. (Alex Bennett, Interview, 2015, 22:18)

Gregory states that institutions are beginning to realize that it is about more than just picking a MDM system and implementing it. Any implementation of a security

system is about configuring the system, setting up rules, knowing your population, grouping devices into lower risk and higher risk devices, and then going back and reviewing that and monitoring the environment.

When asked how he stays up to date with the coming trends and gathers information about security, Gregory stated that:

> We have a security working group that is chartered; and it's the CISOs, Assistant CISOs, and key players on the security teams that are all part of that. And we have a couple of regular discussion forums that are going on. And if I were trying to float a new idea or trying to find out information about where to go to find out about new ideas, that's a group that I would poll first. The second thing that is important is we're part of the Research and Engineering Network - Information Sharing and Analysis Center consortium, REN-ISAC. And we listen to the vulnerabilities as they report them. And we also have a couple of discussion groups on that one from an operational perspective as well as an engineering perspective. And then there is just the idea of a bunch of dudes getting together and sharing stories. I, personally, it's just kind of one of those curiosity things in me. I like to find out about things. So, I spend an awful lot of time in the product sites and seeing what they have to offer; and then I spend probably 60 percent of my time in the vulnerability pages and sites, independent research or maybe targeted research if I'm trying to find out a specific thing. Like, Apple Watch has been the big deal lately; right? And so I've seen the prototype, and that's all well and good and, yeah, wouldn't that be fun? However, I've also looked at the Dark Reading site to see who are already shooting out exploits for Apple Watch. I kind

> of keep a close eye on whatever DHS is putting out as far as alerts and vulnerabilities. And, also, I've read a couple of EDUCAUSE papers. So you have plenty of resources out there. It's just a question of which one do you want to go to and who do you trust? What I really hate is going to a site that says we're going to tell you how to fix this; and it turns out to be, we're going to sell you our tool. You know, and that's just part of the industry. You know, we have to take the good with the bad; right? (Michael Gregory, Interview, 2015, 22:40)

Communications and training.

Though no specific interview question was focused on communication or training, this arose as a theme from each interview. Gregory stated that:

> I would hope that research would bear out that organizations and institutions that have those [security] conversations frequently are less prone to be penetrated. (Michael Gregory, Interview, 2015, 27:52)

While the campus-wide advisory groups are one way that IT information is disseminated, electronic mailing lists, websites, and one-on-one trainings are also used. Occasionally, large-group trainings are used as well. Through all of these communication methods, IT staff, whether centralized or decentralized, seek to inform the campus community about security policies and upcoming changes. All of those interviewed agreed that communication was a critical element in properly securing the environment because end users are the largest point of risk.

When asked about training around security, Gregory stated that:

> One of the pillars of a robust security program is understanding how much training is necessary. We are embarking on a pretty ambitious plan to start

> corralling our users and giving them the right level of training, part of which is understanding mobile security issues. (Michael Gregory, Interview, 2015, 32:05)

While the training is focused on all types of security issues, mobile device security is a component. The training will begin with students, then move to IT and administrators who deal with more secure systems, then will move on to faculty and other administrators. Gregory believes that creating a consistent security awareness program that includes a general Cyber Hygiene overview is important (Michael Gregory, Interview, 2015, 33:00). In order to best address security, a security awareness program should incorporate many different components, not just mobile devices.

In addition to trainings, there are other ways to communicate about security. Gregory stated that "not a lot has really changed because it really all comes down to the educated user" (Michael Gregory, Interview, 2015, 41:45). The more educated they are, Gregory believes, the more an institution's risk is reduced. Gregory stated that:

> One of the things that I am conscious of and I've always remained conscious of is that the learning law of primacy has got to be the most important thing that we pay attention to. If we don't teach them how to do it right from the beginning, then we are never going to be able to change bad behaviors when they start occurring. (Michael Gregory, Interview, 2015, 42:16)

He further explains that it is not a one-time effort. End users need to be communicated with and trained over and over and over again.

Overall, the interview subjects all indicated that the faculty and staff have very diverse feelings on security, and more conversation with them is critical. Communicating

about security issues is a partnership between IT, security staff, and communications staff, according to Gregory. Gregory stated that:

> A lot of folks are tool-oriented; but you have to have a mature enough cybersecurity team working with you that is willing to say it [security] is not just a tool. It's a process and it's people. (Michael Gregory, Interview, 2015, 40:59)

Many want security and understand the needs for it, while others just want their research to work. Each person interviewed indicated that balance was critical and that there needed to be enough security to sufficiently protect the type of data that was being examined but not so much that it would interfere with the critical work of the institution. Determining that requires communication with faculty, staff, and students.

Case Study #4 – Institution D

Introduction.

University D is a small private undergraduate degree-granting institution in the central region of the United States with under 5,000 students and under 400 employees (University web site). The institution is primarily face-to-face instruction with small class sizes and little-to-no distance learning (Cody Grayson, Interview, 2015). Admission into this institution is incredibly competitive, and students enrolled here typically graduate in four years (University web site). Three individuals were interviewed at this institution. Arthur Williams and Cody Grayson were interviewed, and they both work in the IT department. Along with these two individuals, Grace Jones, a faculty member in the field of computer science, was also interviewed.

Environment and staffing.

The following questions were asked by the researcher to assist in creating a picture of the environment at this institution:

- Please describe the role you take in working with mobile devices and/or security at your institution.
- What do you think the perception is of the security of mobile devices by the faculty and staff?
- What do you think your institution does well regarding the security of mobile devices?

Most technology is centralized in the institution's main IT department. With a staff of approximately 30, the IT department supports nearly all of this institution's IT environment. This institution has a newly created information security position that will be coordinating efforts around IT security for all of the campus. Interviews indicated that prior to the creation of this position, security was distributed, and individuals dealt with the security implications around their own specific areas of IT. Arthur Williams indicated that the administration decided that they needed to bring some cohesiveness to the security environment. He stated that:

> As far as security was concerned, it was pretty much handled by the various people depending on their role. The infrastructure person handled infrastructure security, and the apps team had their own kind of security, and I think they got to the point where they just said, "You know, we've got to consolidate security all in one and bring in policies and procedures." I think a lot of pressure was put on

> them by the BYOD. They didn't have a Bring Your Own Device policy in place. (Arthur Williams, Interview, 2015, 00:06)

This position was intended to be one point of reference for all security policies and procedures, as well as a contact for auditors, says Williams.

Williams indicated that the two main priorities for the person in this new security role will be laptop encryption and mobile device security. In discussing the priorities with the President, Williams related a story:

> That got the attention of the president of the college that laptop encryption and mobile device security should be a priority. I think the President was in Washington, D.C. or something and just watched a senator of the United States suffer because, I believe, his laptop was stolen. And he just saw the fallout from it and wanted to make sure it didn't happen. So, essentially, encryption is a priority for him. (Arthur Williams, Interview, 2015, 02:00)

Grayson stated that the trend towards more BYOD at higher education institutions is a large motivator for the institution to address mobile device security and that this will be a major portion of the new hire's role.

When describing the classroom environment at the college, Grayson stated:

> All of our classes are face-to-face and very small. Most, if not many of them, are discussion-based classes. Students don't have a lot of material other than readings and stuff to consume out of class, so they don't rely heavily on their mobile devices for consuming class materials outside of class. I'm sure some do some reading and things like that on their mobile devices, probably more so on a tablet.

> But I guess that almost everything is face-to-face instruction here so it's a lot less here than it is in other places. (Cody Grayson, Interview, 2015, 10:08)

The smaller, face-to-face environment is a unique element to this college, and Grayson explained that the tablet is a tool that he finds fits this environment well. Grayson stated:

> Most of what we've done so far has been based on the tablet format instead of phone or anything smaller because it provides the right balance of functionality and mobility, especially for what we do here. (Cody Grayson, Interview, 2015, 08:45)

Governance and systems.

The following interview questions were asked by the researcher to determine what technical systems, policies, and other frameworks for decision-making were in place at this institution:

- What policies and procedures does your institution have regarding the topic of mobile devices and security of those devices?
- What types of systems do you use to manage mobile devices (example: Mobile Device Management solution (MDM) or something similar)?
- What information does your institution collect about mobile devices and usage by faculty, staff, and/or students?

Though the institution has a more centralized IT environment than the other institutions studied, some items are still decentralized. For instance, there is a central e-mail server for campus e-mail, but certain departments still run their own e-mail services. However, these services appear to be coordinated with the main IT department (Grace Jones, Interview, 2015).

In terms of the mobile device landscape, there are very few institutionally-owned mobile devices. Williams indicated that, in some cases, this makes controlling the environment a bit easier because there aren't many devices to manage yet. Williams stated:

> I'm kind of fortunate in the sense that mobile devices, we don't have that many currently, and we don't issue the phones at this point. So I have some breathing room to get stuff established before we start doing that. (Arthur Williams, Interview, 2015, 02:00)

This will enable the institution to prepare policies, procedures, and systems to help manage these devices before they are purchased with University funding. There are a few small areas that share or check out a few iPads, and only a small handful of staff have institutionally-owned smart phones. Cody Grayson indicated that the iPads are not managed by a mobile device management system, though they are reset between uses, and end users are not storing or retaining any data on those devices. When discussing how faculty use the iPads, Grayson stated:

> Basically the way that we've done it is, we have this cache [of iPads] and when need arises, we try and use the ones that we have. We just pretty much wipe them when we get them back and hand them off reset so that people could use them to set up their own profiles. We don't manage very many apps, so we've purchased very few apps for those iPads. We haven't really gotten into purchasing more apps for faculty on a big scale. We've just done one or two here and there. But on a large scale, we haven't. (Cody Grayson, Interview, 2015, 01:38)

This institution does not have a mobile device management solution, but it is exploring one for use in the future. This institution does use a central e-mail server that can act in some small capacity as an MDM if the institution chooses. This central e-mail server can provide remote wipe capability, if the institution chooses to use this feature. However, this institution does not have a policy around any other security rules around these devices such as encryption and passcode.

This institution does not collect information about specific mobile device usage. However, they are working on implementing a system to collect data about who visits the web site, what type of devices they are using, and the demographics of visitors to the institution's web site. This does not provide data on what other types of things faculty, staff, or students may be doing with mobile devices.

By and large, the interviews indicated that faculty and staff who are using a mobile device are using their own personally-owned mobile devices. The interviews indicated that faculty and staff are mostly using mobile devices simply to check e-mail, with no known cases of classroom instruction that integrates the usage of these devices. The interview subjects indicated that connecting faculty and staff to e-mail is easier to support than the variety of other classroom instructional uses that may arise and that if faculty began to explore using these devices in the classroom more, additional staffing resources would likely be needed.

Interview participants indicated that the faculty population, in general, does not spend a great deal of time thinking about security of their mobile devices. Jones has been a faculty member in the field of computer science at this institution for several years and stated, "I would guess that most people just don't think about it. To be honest, even I

don’t most of the time” (Grace Jones, Interview, 2015, 07:03). Jones indicated that faculty are much more concerned with their classes and their curriculum and that security is not typically something at the forefront of their mind.

There are many IT policies in place at this institution. Policies that exist revolve around how students, faculty, and staff may use the institution’s account, network, and computer resources, but there are not specific policies dedicated solely to the usage and security of mobile devices in particular. Williams indicated that the institution has procedures around PCI and FERPA data and follows those policies set forth by the federal government. When asked about a data classification matrix or policy, Williams replied:

> That currently is not in place. Since the day I started, I've been hammering on it. And I'm not really picky about how they define it, whether sensitive, confidential. The only thing in place right now is the obvious ones like the PCI and FERPA are pretty well known around here. But I asked them, "Well, what about research? How about student’s grades, laptops that are encrypted, social security numbers, all of that kind of stuff?” The data classification, I'm not really sure at this point if that is my role entirely because I wasn't hired as a privacy officer; I was a hired as a security officer. And I’m not a compliance officer either. The only problem is, there isn’t a privacy officer; there isn’t a compliance officer. So I feel like my role might be expanding here. (Arthur Williams, Interview, 2015, 04:52)

The institution is working on a new confidentiality agreement, according to Williams. Student, faculty, and staff will have to sign upon entering the institution to

indicate that they are aware of the IT web site and the policies and procedures around institutional data and their usage of institutional accounts. Williams stated:

> We're doing something with students as part of their onboarding process. They're going to have to sign a confidentiality statement. They're going to have to be aware that there's a website dedicated to security and that they need to be cognizant of it regardless of whether they're using [the institution's] equipment or their own equipment. They have certain responsibilities that they have to adhere to. (Arthur Williams, Interview, 2015, 18:32)

Williams is starting with students first, but believes this is a critical step towards making sure that students, faculty, and staff are aware of both the resources offered on the IT web site and the policies they must follow to help keep the institution secured. "You really just have to have some solid policies in place and training available to implement those policies" (Arthur Williams, Interview, 2015, 13:15).

Future plans and trends.

The following interview questions were asked by the researcher in order to determine the interview subject's perspective on the direction of mobile device security, both at this specific institution and in the industry at large:

- What trends do you see coming in the future regarding mobile devices and/or security?
- What do you think your institution does regarding the security of mobile devices that needs improvement?
- What resources, processes, policies, et cetera do you wish your institution had to assist with the security of mobile devices?

The experts interviewed at this institution stated that some trends that are coming in the field of technology include bio-authentication technology and password management software. With bio-authentication, end users use their fingerprint, their face, or even their eye to access and unlock their device or their data. Jones indicated that Apple is already going this route with their fingerprint scanning of iPad devices, but other companies are adopting these security measures as well in order to provide greater assurance that no one can obtain unauthorized access of someone's device or data. Jones stated:

> A place where this really touches on my area of specialty would be how people interact with security systems. And in terms of any sort of trends I see there, I think bio-authentication is definitely coming. We've already got it with the iPhone, the little touch pad on the iPhone, the fingerprint reader. (Grace Jones, Interview, 2015, 03:03)

Grace Jones stated that password management technology, or a password safe, creates passwords "which are much more secure than passwords I would generate on my own" (Grace Jones, Interview, 2015). She further explains that:

> I started using a password safe after I started using a mobile device, meaning a piece of software that stores my passwords in a cryptic form, and it automatically enters a password for me, which are much more secure than the passwords that I would generate on my own. I hope that's a trend, because I think so many systems and websites require the use of passwords now, that I think it is literally impossible for a human being to remember all of the passwords unless they use

> the same passwords over and over again, which, as we know, is problematic in its own way. (Grace Jones, Interview, 2015, 04:00).

Reusing passwords over and over is a major security risk because it means if one account is breached, you are risking exposure on all of the other accounts as well. Because passwords are used so extensively and best practice means they should be unique to each web site, some people prefer the ability to store them on their mobile device. People typically carry their mobile device with them everywhere, and this means they would have all of their passwords with them anywhere they go. However, this also means that if an individual loses their mobile device or it is stolen, the person who finds it or steals it would potentially have access to all of that individual's passwords as well. This increases the need for security on those devices, as risk rises exponentially when all of one's authentication records are stored on that device. Jones states that, as this trend of password management grows, so do the risks, and it becomes increasingly important that the device have a stronger level of password protection or bio-authentication. Jones stated:

> I guess having the bio-authentication or multifactor authentication, I think that's always on trend. I think the password safe is a trend because you've got your mobile phone with you all the time, so that makes it much more practical to have a secure password saved. (Grace Jones, Interview, 2015, 04:47)

When asked about trends in mobile device security, Williams stated that he is more concerned with internal threats to IT security and not as much worried about the external hacker. The people are what concerns him, and he is not as worried about the devices. Williams stated:

> You know, I'm not sure if the Russian hackers are who I'm worried about. What I'm worried about is the 18-year-old college student who gets a 35 on their ACT but still lacks common sense. And so I'm probably more concerned with internal threats. (Arthur Williams, Interview, 2015, 10:47)

He further stated:

> I kind of think of my job as preventing people from making dumb mistakes, and I'm less concerned with things getting stolen out of cars or cabinets and stuff along those lines, although that's a possibility. Yeah, [I worry about] the obvious stuff like sending classified, confidential information to the wrong people, the wrong e-mail addresses, stuff along those lines. (Arthur Williams, Interview, 2015, 12:37).

When asked about trends in mobile device security, Grayson indicated that a growth of tablets is likely coming. Grayson works in an area of IT that assists faculty in their coursework and states that classes are small, discussion-based, and not often lecture-based or auditorium-style classes. Almost everything is face-to-face, according to Grayson. Grayson states that:

> The tablets get used, and I think those will continue to be used and will probably get more and more use as the software gets better. The sharing will get more and more. In discussion-based, there's a lot of peer work or group work, and the tablets are good at facilitating that. So I see that growing here. (Cody Grayson, Interview, 2015, 11:04)

Because of the uniqueness of this institution's emphasis on face-to-face classes and peer work, tablets have a unique role to fill and are expected to grow in usage.

Communications and training.

Though no specific interview question was focused on communication or training, this arose as a theme from each interview. One of the first items that is being targeted to address within mobile device security is creating a security awareness program for end users. There are IT staff who conduct training for campus, but Grayson stated that he doesn't typically observe faculty requesting mobile device or security-related training (Cody Grayson, Interview, 2015, 14:17). Williams indicated that there is not a current training curriculum around IT security at this time, though future plans include the development of a security awareness program. An option for a training curriculum that Williams has used in the past and is examining for use at this institution is the SANS Securing the Human training found at www.securingthehuman.org. Williams stated that this is a popular choice among higher education institutions for educating end users on security. This training curriculum is not limited to mobile devices, but much broader. It seeks to change user behavior and reduce risk to the institution.

Though there is no specific awareness or training program right now, Williams stated that this is a priority. Williams stated that in the past:

> One of the biggest areas that was neglected was just an awareness program. So I'm creating a site and probably going to work with the SANS Institute. We had good luck in my previous work with an awareness training program called Securing the Human. (Arthur Williams, Interview, 2015, 03:27)

Grayson also indicated that communication about security could use some improvement, stating that:

> I don't know that we do anything really poorly, but I guess I would say that to know that we are doing it [mobile device security] really well, it would have to be something that we talk a lot about, or that we communicate a lot about. I just don't feel like we communicate a lot about it, either within ITS all that much and especially not with the campus at large. (Cody Grayson, Interview, 2015, 12:33)

Grayson indicated that the hiring of the new security person was fulfilling a need to help communicate more about security.

Cross-Case Analysis

Everyone interviewed agreed that end users are the largest point of risk, no matter what the institution or the situation. End users have a variety of devices, habits, and uses, and security is not always at the forefront of their mind as they seek to use their devices to complete their work. Because security is not always a consideration for these faculty and staff, their habits present a large risk. However, it is important to note that students were not frequently brought up in the interviews as a high point of risk. It was clear that the interview subjects considered faculty and staff a higher point of risk than the student population. Faculty and staff were frequently brought up as risk points because of the types of systems and confidential data to which they have access.

All institutions were using or in the process of switching to a centralized cloud-based e-mail system which has the capability to act as a "light" mobile device management system, allowing the institution to remotely wipe devices, enforce passcodes, and require encryption of the device. No institution examined had an over-arching robust MDM solution in place.

Table 2

Systems at Each Institution

	Institution-wide MDM	Cloud-based E-mail	Using the Cloud-based E-mail "Light" MDM Features
Institution A	No	Yes	Partially
Institution B	No	Yes	Partially
Institution C	No	In Progress	In Progress
Institution D	No	Yes	Partially

Three of the four institutions were using the centralized cloud-based e-mail system as a light version of an MDM today, using at least a few of the tools available within that system. However, every institution is exploring the possibility of using more of those features in the future. It is important to note that some interview subjects felt that the less intrusive security features of the cloud-based e-mail system were actually a better fit for their institutions than a more restrictive MDM solution.

The two larger institutions had a much stronger focus on faculty research data and protecting potentially confidential or restricted research data, while the interviews from the medium-sized and smallest institutions did not reflect that same need.

Every institution indicated that communication and a security awareness program was critical to the success of any security initiative. All subjects interviewed indicated that policy is critically important and that their institution could use more policies to assist in clarifying the security around mobile devices. Two of the four institutions had a clear and well-defined data classification policy, but the remaining two institutions indicated that it was a clear need to develop one in the future.

Table 3

Policies at Each Institution

	Institution-wide Data Classification Policy	Policy Addressing Mobile Devices Specifically
Institution A	In Progress	In Progress
Institution B	Yes	Yes
Institution C	Yes	Yes
Institution D	In Progress	In Progress

Another theme that emerged from the interviews was a lack of resources. Interviews indicated that mobile device security is not something that most faculty, staff, and students are thinking about on a daily basis. Because of this, obtaining funding or resources for security initiatives can be difficult because it is easily ignored until an actual breach occurs. One interview participant indicated that funding seemed to be sufficient for current security initiatives, but all of the other interview subjects indicated that more resources for training and/or technical work would be extremely helpful towards making their institution more secure. When discussing widespread security mandates and the repercussions, Douglas stated:

> We [higher education institutions] all have such diverse needs and such diverse staffing levels. I can imagine that it would be incredibly hard to comply with some of those things, based on the resources that they have. (Everett Douglas, Interview, 2015, 2/09:44)

As demands continue to grow around mobile device security, Jackson stated:

> The problem that we have with our network environment right now is we only have two guys that can do that, and they are completely overwhelmed. We need a third person and over the past year have been unable to add that person that can focus on security and better management. So right now, we're just completely strapped by resources. (Luke Jackson, Interview, 2015, 12:10)

This is an important barrier of which institutions need to be aware.

One interview protocol question that did not garner much information was:

- Describe an incident or issue regarding mobile device security that your institution has faced recently.

Interview subjects struggled to come up with an example of a specific security issue or incident relating to mobile devices. The few interview subjects that could come up with an example cited small issues with little to no real impact to the institution. Gregory stated, “Not serious issues” (Michael Gregory, Interview, 2015,17:00). Adamson stated:

> It's not necessarily a mobile device, but we had a student laptop stolen. So we had to track it. Once it's stolen, it's really difficult to track down. We were able to track its movement across campus, but once it leaves campus, we don't have any more visibility into it. (Kurt Adamson, Interview, 2015, 08:57)

Kevin Johnson stated:

> I don't have any specific mobile device. Oh, actually, I do. I had a mobile device stolen from me. I actually had an iPad go missing. So we actually have a security response methodology that we follow from our help desk that involves us contacting, immediately, our IT security department. I believe the first thing that they do is they actually will speak with the end user to determine any risk for data

> that may be on that device, for example, if it's a lost laptop or something along those lines. Then they actually will work to perform whatever risk mitigation they can. For example, the device that I lost, I had essentially no data on it. I didn't connect it to campus e-mail. The only thing that I did was connect it to campus wireless resources, so I had no data actually stored on the device. Their response was, "Okay, you need to just contact the police department and fill out a loss form." And they guided me through that process. (Kevin Johnson, Interview, 2015, 10:24)

It is difficult to speculate as to why there were few examples of mobile device security issues. It could be that their role is not made aware when incidents occur, that incidents are not occurring at all, that incidents occur but are not reported to IT, or a variety of other reasons. Though it is unclear why, it is important to note that there were not ready examples of mobile device security breaches occurring at the time of the interviews.

It is interesting to note that all institutions have newly formed, newly re-organized, or newly created security leadership positions, such as a CISO or security manager, which could be indicative of the growing emphasis on IT security in higher education. All institutions indicated that it is critical that these high-level IT security roles have a seat at the table with campus administrators in order to ensure that security is well-planned and aligns with the business needs of the institution.

Though there were a variety of methods, each institution had methods for employees, students, and guests to access the wireless network using their mobile devices. Interview participants indicated that because visitors and guests to campus are

part of the business of running a higher education institution, it was critical to provide this service even though guest access can sometimes create a security risk.

All interview subjects agreed that access needs to be balanced with security in order to ensure that the business functions of the institution as well as the research mission of the faculty can be completed. Interview subjects aligned on the fact that it is difficult to obtain that right balance but that communication with the campus community makes it easier to find the right fit for the institution's individual needs.

CHAPTER 5 – DISCUSSION AND CONCLUSIONS

Introduction

The interviews conducted have led to many interesting findings, and, in some cases, more questions to be answered. First, the researcher discusses the key findings that emerged from the research study. Next, as an additional way of addressing the research questions, the researcher has formulated several key recommendations or "best practices" that institutions should consider as they approach their mobile device security strategy.

Key Findings

Table 4

Mobile Device Themes from the Research Study

Themes specific to mobile devices
Mobile device security is a growing problem.
There were no current examples given of significant security breaches related to mobile devices.
It is critical to protect the data and network, not try to control the mobile device.
End users are the biggest security risk.
Faculty and staff pose a significantly higher risk than students.
A data classification policy/standard is foundational to mobile device security.
A security training or awareness program is critical to mobile device security.
It is critical to balance security with an appropriate level of access.
The topic of security is much bigger and difficult to limit to just mobile devices.

Table 5

General Themes from the Research Study

Themes general to all IT security
The mission of higher education is different from the mission of the private sector, and that impacts security.
Three of the four institutions interviewed had newly created or newly restructured CISO or CISO-like positions.
Frequent communication with and involvement from the campus community is critical to success.
It is critical to get buy-in from administration on security.
Security is the responsibility of the entire organization, not just IT.
Other IT staff need security training, not just the CISO.
There is a lack of staffing & financial resources dedicated to security.
Do not adopt a standard in totality, but use it as a starting point and customize it to the institution's unique needs.
It is critical to have a security plan or roadmap.
There are security organizations that can provide value and expertise.

The researcher formulated one main research question with four sub-questions that were sought to be answered by this research study:

- How have four higher education institutions responded to the threats to campus data security posed by mobile devices?
    - How are the selected higher education institutions in the Midwestern United States addressing mobile device security today?
    - What policies and procedures surrounding mobile devices have the selected universities established?

- How are the selected institutions balancing the question of security versus accessibility and usability?
- In what ways can leaders proactively handle security challenges that will be brought on by mobile devices in the future?

The case studies presented create a picture of how each institution has responded to these mobile device security threats at the time the study was conducted. The case studies outline the way that that particular institution is addressing mobile device security and what policies and procedures they have in place at the time that this study was conducted. Baker and Wallace (2007) stated that "Technical approaches alone can't solve security problems for the simple reason that information security isn't merely a technical problem" (p.37). The full picture of how to address security at higher education institutions must include technical solutions, policy creation and review processes, communication strategies, and much more. As institutions seek to develop a strategy or adapt their current strategy, both the literature studied and the interviews led the researcher to the conclusion that the most important themes from the research study are:

- IT needs to communicate.
- A security awareness program is critical.
- Balance control with access.
- Increased resources are needed.

An important finding of this research study was discovered before any interviews even took place. It was clear as the researcher was approaching interview participants that many potential participants were intimidated or afraid of the research study because it dealt with mobile device security. Security is a scary topic, the researcher found. Even

though the researcher believed many of the questions being asked were very high-level and did not pose a risk to the institution, many individuals approached were worried that something they would say would lead to a breach or would paint their institution in a negative light. Others expressed that they simply did not know enough about the specific topic because it was a newer consideration for their department. Though exact data wasn't tracked, over 30 participants declined to be interviewed. Of the research participants that did agree to participate, the researcher found a wonderful openness, a willingness to help, an excitement about partnering with faculty and staff to create an improved security environment, and a vast base of knowledge that was invaluable to this study.

Another clear finding from the interviews was that it was difficult to limit the discussion to solely mobile devices. First, there are many overlaps in technology. For example, the same technology that one uses to access e-mail from a mobile device is also used to access e-mail from computers. Second, the types of techniques that one uses to protect their mobile devices may have impacts for all devices on campus. An example of this is a firewall, which can protect not just mobile devices but also all computers inside the firewall. While protecting things inside, it can also limit some of the types of academic research that need to be completed because it may block out legitimate things as a consequence of having the firewall in place. Even though a solution may be needed for mobile device security, it may have farther reaching implications than intended, so each measure of mobile device security needs to be examined closely before being implemented. Third, many of the things discussed in the interview were actually much larger than just mobile devices alone. The funding, policies, and user education items

needed to protect mobile devices can often apply to the entire institution. For example, developing a data classification policy is one of the key items needed to help end users to understand what data they can and cannot access from their mobile device, but this policy also assists the institution in how to handle all types of institutional data from all types of devices, not just mobile devices.

Though this research study focused on faculty, staff, and students and the mobile device security for all of those types of audiences, the most frequently discussed group by interview subjects were the faculty and staff populations. Students were rarely mentioned in the interviews as a point of risk. The researcher proposed that this may be because they typically have access to so little institutional data. It is likely that the perception of the risk students introduced was considered minimal when compared to the risk introduced by the access to institutional data that faculty and staff have today.

When interview participants were asked to cite examples of mobile device security breaches or problems, there was difficulty in coming up with examples of significant impact. Despite this, every interview participant acknowledged that this is a growing segment of the industry that needs to be addressed, and much of the interview conversations revolved around what needed to be done in the future. Resources were frequently brought up as an important component, both from a financial standpoint and a staffing standpoint. It was often raised as a barrier when there were not enough resources dedicated to security.

It was apparent that the final sub-question which discussed how leaders can proactively handle security challenges in the future was a very important consideration for those interviewed. Additional involvement with the campus community is absolutely

critical to the success of these endeavors. Though the policies and procedures are varied, there was a theme throughout the interviews of needing a data classification standard as a foundational piece of the mobile device security puzzle, as well as other policies and procedures in order to better clarify support and expectations for mobile devices across the entire campus. Having a security plan or roadmap in place was found to be the most important way that institutions can prepare themselves to address the security risks of the present and those coming in the future.

An important finding of this study was that three of the four institutions examined had a newly created or newly restructured Chief Information Security Officer position. This suggests that institutions are recognizing the importance of security and are striving to create a position that can address these growing needs. What is currently unknown is the skillset that will make a CISO position successful in the higher education environment.

The researcher conducted some of the literature review several years ago which enabled a unique perspective on the research topic. Several years ago, the literature reviewed was pointing towards control, control, control. The literature advocated for adding mobile devices into an MDM system and controlling the devices as much as possible. However, current literature advocates that IT departments focus on controlling the data, not the devices themselves. The interviews supported these literature findings but demonstrated there is still much more work to be done to secure mobile devices.

Looking into the future, the institutions studied are continuing to adapt their strategy as technologies evolve. The below best practices were created by the researcher to assist higher education leaders in preparing a strategy around mobile device security.

While the below best practices specifically refer to the topic of mobile device security, many extend far beyond that individual topic and apply to an institution's security structure overall. These best practices are:

- Ensure that security risk is part of the conversation with the entire institution.
- Communicate and market security to the internal community.
- Balance control with access.
- Protect the data, don't control the device.
- Conduct and utilize a gap analysis.
- Employ a data classification guideline or policy.
- Implement a security awareness program.
- Move the conversation up a level, and make sure it's the *right* conversation.
- Grow all IT professionals in security skills, not just identified security professionals.
- Connect with leaders in other venues.

Ensure that security risk is part of the conversation with the entire institution.

Brechbuhl, Bruce, Dynes, and Johnson (2010) stated that "if you are on the network, you are available to everyone else on the network. A key consequence is that security is not the concern of someone else; of necessity it is the concern of everyone" (p. 84). Security risk is not just the IT department's problem. This statement may seem quite obvious, but it was clear through the interview process that it is not yet the case in some of the institutions examined in this research study. Those interviewed were passionate

about how important clear communication with the campus community was to the success of any security initiative. Bennett stated:

> The more that that [policy] can be discussed and that there's an opportunity for the wider campus to participate in the conversation, the more successful the outcome can be. (Alex Bennett, Interview, 2015, 20:11)

All four of the institutions studied have communications departments within the institution and work with those departments to share messages with the campus community. Institution C states that they "have a campus communications team, and we work with them quite well to do things like the IRS tax fraud scams that are going out right now" (Michael Gregory, Interview, 2015, 35:53). In addition to the campus communications, Institution C also has "a communications team inside the department of IT" to assist (Michael Gregory, Interview, 2015, 35:40). Douglas stated:

> We have to learn to better communicate, to better integrate, so that it [IT security] doesn't end up something that we try to bolt on at the end and then nobody else is happy with us. And faculty members play a key role in this. (Everett Douglas, Interview, 2015, 1/09:30)

Douglas advocates for faculty involvement early and often in order to improve the successful implementation of technology security initiatives.

Something frequently brought up during the interviews was confusion over the responsibility of IT security and the risks associated with it. This was not something frequently presented in the literature, but was clearly articulated in the interviews. There was often a question raised about how IT departments make the upper administration care enough about security to invest in it *before* a breach occurs.

It was not always clear whether security was the primary responsibility of the institution as a whole or the IT department. Many institutions who have a designated CISO or Security Manager position assume that this person is responsible for the risk and is held culpable if a breach occurs. Speaking of his own role as a CISO, Adamson stated that the driver behind creating his position was to provide “a higher-level authority, ensuring that security's made a priority for the campus” (Kurt Adamson, Interview, 2015, 01:13).

Sometimes the IT security position(s) resides within IT and sometimes outside of IT, which can impact how responsibility for security is viewed within the organization. Douglas stated:

> From a trend perspective, this is another one of those where things are changing in the commercial sector. There are an increasing number of CISOs hosted or housed in places other than the CIO, so they might be put under the CFO. I've noticed a CISO who was reporting directly to his CEO for a while. In some cases, they're put under chief risk officers or even legal. And so, that creates different lines of communication and reporting, and so that structure is key in a way, that governing structure, that organizational structure. (Everett Douglas, Interview, 2015, 1/19:23)

It could be argued that moving the CISO up a level to report directly to the President may make it a more effective position because that person would have direct access to the President for funding and decision-making, as well as a seat at the table during important institution-wide decisions. Having the CISO report directly to the CIO may be a conflict of interest, “because in a way, the business side is not on board or the

IT filter ends up getting in the way" (Everett Douglas, Interview, 2015, 1/21:14). If obtaining resources for systems or support is in direct competition with dedicating resources for security initiatives, sometimes security may lose out in the process.

However, because of the political climate at many higher education institutions, arranging the organizational structure to allow the CISO to report directly to the President may be problematic and controversial. An alternative to consider may be having the CISO reporting outside of IT such as to a risk management department.

Obtaining additional resources for investment in security may be difficult today. Yet if the higher level administrators understand just how much of the risk they shoulder themselves, it may be easier to obtain those resources in the future. Both the literature and the interviews indicate that obtaining funding and staffing for security is often difficult because it is an unseen problem (Imgraben, Engelbrecht, & Choo, 2014). Institutions seem to believe that it is the CISO position that is ultimately responsible if something goes wrong. Interviewees discussed how this perception sometimes makes it difficult for the CISO to obtain funding to solve security issues. However, one of the interview subjects presented an article that challenged this assumption that security is the CISO's problem. A 2015 study conducted by NYSE Governance Services in coordination with Vericode demonstrated that the CEO of the company is actually the first person held accountable when a security breach occurs. In the case of higher education, the CEO is typically considered to be the President of the institution. Next in line is the CIO and the entire executive team, followed by the CISO position. One item of note is that members of a governing board may also be held accountable when a security breach occurs.

It is important to determine who holds the risk because often garnering support for IT security resources can be a challenging prospect. If administrators understand that they also hold some of the risk, there will be a greater likelihood that they will care about the security risks, take an active role in the security planning, and invest resources and funding into securing the environment.

So who owns the risk? Everyone. The researcher suggests that institutions will have a higher rate of success with security initiatives if they dedicate time and resources to convey to all of their constituents that security is important to everyone.

Communicate and market security to the internal community.

Often institutions of higher education are familiar with marketing services to prospective students, but it can be challenging to think about having to market security services and information to internal faculty and staff. Yet marketing and communications are a critical and often overlooked piece of the security puzzle. This research study demonstrated that end users are the biggest risk and often unaware of security needs, practices, and requirements. That is a dangerous combination. Institutions need to "sell" security information and services internally. Douglas stated that:

> Even today, even with the thirst, even with the demand from the higher ups -- the executives getting the same message that security is important, but it still has to be sold as a concept. (Everett Douglas, Interview, 2015, 1/12:10)

Institutions need to help end users understand why it is important to care about security. If this is not done, end users will continue insecure habits and practices, further exacerbating the security risks for an institution.

As a part of the communications and marketing strategy, it is important to ensure that IT security personnel are positioned for success. Often IT security employees are hired for their security expertise. However, that is not always the most important factor when it comes to a successful security program. Yes, technical skills are needed for the back-end system work. However, for the security manager or CISO, the much more important skill is how they communicate with the campus community. In discussing hiring a security manager-type role, Samuels stated “these are very hard positions to fill” (Victor Samuels, Interview, 2015, 16:30). The person in this role needs to be able to evangelize the security plan to a non-technical audience. Because this plan is often complex, costly, and boring to a non-technical audience, this requires a unique skill set. It is important that this role is hired appropriately. Douglas stated an example of this:

> One of our security people was briefing a whole group of faculty from my college, and in the process of talking about some of the things they were concerned about, this person started spewing out a whole bunch of security technology acronyms. And the faculty members starting glazing over, and so finally I raised my hand, and I said, "Here's an analogy. It's kind of like you're about to buy a new car. You bring it to a repair shop, and you have them do basically a full rundown of anything that might be currently wrong with the car or might be needed in the next six months." And, suddenly, we got reengaged in the conversation. In a way, it's about conversation and communicating using the right metaphors at the right time with the right audience. (Everett Douglas, Interview, 2015, 1/14:25)

This research study also demonstrated that IT is often not fully aware of what faculty and staff are doing with their mobile devices. Making heavy-handed security policies without involving the campus community is sure to garner negativity and resistance. Douglas stated:

> About a year ago, they [the IT department] set out to push a policy update to enforce screen locks, screen savers with password locked, and when they presented this to faculty union, they really were not prepared for the amount of pushback they got. They actually had to basically table their plan to deploy this and come back and really explain, why are they doing this? What is it that is going to help mitigate in terms of risk? What are the exception policies? Because, initially, they hadn't planned for much of that. And, to me, that's very representative of this disconnect. (Everett Douglas, Interview, 2015, 1/10:27)

Another reason communication is so critical is not just to get buy-in, but to prepare for exceptions and to create a better end result that does not inhibit the mission or business of the institution. Douglas stated:

> It would be much more advised for technologists to really partner up with representatives from faculty and other groups to be a sounding board to get some feedback before they start launching some kind of change, because people are reluctant to change, and faculty members are super reluctant to change. (Everett Douglas, Interview, 2015, 1/13:30)

Adamson stated about security:

> It would have to be relevant to them [faculty]. They don't want to have to think about it. They just want to be able to do their work, teach classes, and not have to

> think about mobile device management. We need to make it as transparent to them as possible. I think most of them are sort of aware of it in the back of their minds. They don't think about it on a daily basis. (Kurt Adamson, Interview, 2015, 20:23)

Remember, communicate, communicate, communicate, and "if you think you've communicated enough, double it, and then double it again." (Matthew Hudson, Interview, 2015).

Balance control with access.

Higher education institutions have needs which are distinctive from the needs of the private sector. Connections can be drawn across environments, but standards created for the private sector should not be unilaterally applied to higher education institutions. While higher education leaders and IT professionals can learn from the private sector, these two environments are NOT exactly the same. Access and flexibility are often more critical in higher education than in the private sector. Weston stated that "All they [faculty] really want to do is do research, and they want that to be as easy as possible" (Dylan Weston, Interview, 2015, 13:54) Many faculty and staff expect to be free to do their jobs, and this expectation, while many argue the nuances, is not going away any time soon (Michael Gregory, Interview, 2015; Everett Douglas, Interview, 2015; Kurt Adamson, Interview, 2015; Luke Jackson, Interview, 2015, Dylan Weston, Interview, 2015). When asked about implementing mobile device security policies or restrictions, Adamson stated:

> It's really hard to do in a higher educational institution with faculty having academic freedom and with faculty really owning their content and where that content ownership line is. (Kurt Adamson, Interview, 2015, 04:26)

It is critical to the success of a program that this be recognized and built into the planning. Any action that can be seen as threatening academic freedom will create unnecessary pushback.

Joel (2010) recommends that:

> Rather than imagining using a scale to weigh security interests *against* liberty interests in forcing an either/or choice to approve a new technological capability, consider viewing the scale as a means to determine the "weight" that is needed on each side to *keep the scale balanced between security and liberty*. Our focus should be not on which side outweighs the other to inform a go/no-go decision. It should be on giving *equal weight* to security and liberty interests affected by the technology so that the scale *remains balanced*. (p. 1756)

Gregory stated that:

> We can go out, and we can get all the whiz-bang mobility-enhancing devices that help keep things protected. But, if we are going to slow the rate of research by causing excessive VPN connection times and stuff like that, then we're not helping. (Michael Gregory, Interview, 2015, 39:50)

Interviews showed that many institutions are using their cloud-based e-mail solutions to act as “light” versions of MDMs. This solves two problems: a lack of funding and a need to impose minimal controls so as not to aggravate the constituents or hinder academic research. Using these systems (Office 365 and Google being the two most

popular) allows institutions some minimal control to enforce passcodes, encrypt devices, and remotely wipe lost or stolen devices. This seems to be something that fits that right mix of controls and access. Because those options are typically free or already included into an institution's license, this is a cost-friendly alternative to the extremely high-priced but more robust MDM solutions.

One concern of using any of these systems, even in a light capacity, is that many individuals interviewed noted that they did not believe faculty were fully aware of the capabilities of these e-mail systems (Victor Samuels, Interview, 2015; Everett Douglas, Interview, 2015). It should be noted that using a "light" form of an MDM is not an excuse not to communicate. It is just as important to communicate the capabilities of these systems to the end users as it would be to communicate the implications of a robust MDM.

As we examine other implications that could affect access, such as policy, firewalls, and other security initiatives, it is always important to weigh the costs versus the benefit. The costs are not just monetary, but also include employee time, perception, and other harder-to-measure soft costs. This was not something found in the literature reviewed, but was clearly articulated in the interviews. "Never impose a countermeasure where the cost of that countermeasure is going to exceed the value of the resource" (Michael Gregory, Interview, 2015, 39:35). If the product is too restrictive, if it inhibits the business of the institution, it may not be worth it. Gregory stated that faculty "want as much security as is necessary to keep education running but not more security that would be intrusive and halt what they are doing in the classroom" (Michael Gregory, Interview, 2015, 10:42). Communicating with campus stakeholders will assist in determining which

solutions have the right mix of usability and security to enable the institution to be successful.

Protect the data, don’t control the device.

Protect the data, don’t control the device. Make this the mantra of the IT department. These days, devices are becoming interchangeable. The interviews demonstrated that some end users are likely not even storing any data on their devices at all anymore because of the mass adoption of cloud storage. People are using those devices to log into a variety of systems, and there is very little data available about what they are doing or to what resources they are connecting at most institutions. Brooks stated:

> I think we’ve done well protecting the data, not the devices. That’s kind of made the devices a little bit… I mean, they are an incoming vector, but they are just another one. There are some unique aspects to it, but as long as we are protecting the data that actually has the most risk, I worry less about the endpoint. (Duncan Brooks, Interview, 2015, 13:48)

It is an insurmountable task to attempt to locate and restrict all mobile devices, especially when new devices enter the environment on a daily basis.

Bennett stated:

> The devices will continue to change, and the other thing is because of the diversity. There's not like an enterprise architecture where you can close down, require people to use specific devices or they don't get access to the network. It's an open environment, and you basically have to move the security more into the

> network rather than on the device itself from our perspective. (Alex Bennett, Interview, 2015, 13:56)

Protect the data at its core by ensuring that systems that are accessible online are secure. There are various methods to accomplish this, such as two-factor authentication (which is growing in popularity), registering devices to obtain increased access to systems, restricting data to only be accessed from the on-campus network, and many more. Further research is needed on this topic to determine the appropriate methods, but the thing to remember is that the device that is being utilized is becoming unimportant.

Conduct and utilize a gap analysis.

The interviews illustrated that addressing mobile device security should be one component of the larger security plan for the institution. The first step in developing a security plan is knowing what the security risks are. Some institutions interviewed were working from a common standard, such as the SANS Top 20, but such a standard is only a starting point.

Speaking specifically of the SANS Top 20 Security Controls, Adamson stated:

> It will have some recommendations. It's not specific to higher education, but it's very general. And we're not going to achieve, there are many areas where we will never achieve 100 percent. It isn't realistic in our environment. But we have to decide, "Okay, given this area, given what this document says, what can we achieve? What's realistic?" (Kurt Adamson, Interview, 2015, 14:39)

Before an institution can develop a security plan, it is important to know where the gaps are. Every institution is unique, and, as Adamson's interview indicates, higher education is unique. Leaders need to ask themselves, what are the points where the

institution is the weakest? What are the points of biggest risk for the institution specifically?

An institution should not just adopt NIST, ISO, or some other standard because it won't necessarily fit the specific needs of the organization. A review of web sources surrounding Institution A revealed that Institution A had mandated the use of the ISO 27002 security standard across all institutions. This decision came from an over-arching governing body but was not discussed with the individual institutions within the system. Douglas stated that this mandate likely did not fit the needs of each unique institution; there was no plan or funding regarding how to address it, and no one was "bought in" to the standard (Everett Douglas, Interview, 2015, 2/08:12). The researcher predicts that there is a high likelihood that the Institution A will not be able to reach the goal of compliance with the mandated standard because of a lack of resources and a lack of buy-in from the institution. More importantly, as they work towards compliance, they will be expending valuable resources, both financial and staffing, working on items that may not be their highest risk for a security breach. The cost of IT security initiatives is high, and with only so many resources to go around, it is important to focus on the specific weaknesses of the institution and not waste time and money securing things that are not high risks to that particular institution. Douglas stated that this "edict" about the ISO Security Policy 27002, is problematic because he sees this as:

> A whole bunch of unfunded mandates where [the governing body] is going to make decisions and push things down, and suddenly the campus leadership is going to be on the hook. If I'm the campus CFO, the campus vice president, and the campus president, from an ISO 27002 perspective, all of these folks would

> have to sign off on everything. They have no clue that this is happening. It's kind of like a train headed straight for them. (Everett Douglas, Interview, 2015, 2/09:00)

These issues all point to a strong likelihood that the adoption and implementation of this standard will not be successful. Using a standard like SANS Top 20 or NIST is a good place to start, but institutions need to tailor their strategy around their particular needs. Adopting a specific standard will just mean a lot of resources thrown at problems that may not be that particular institution's biggest risks.

The gap analysis needs to include interviews with IT and non-IT personnel, not just a review of the systems. It is critical that the voices of the faculty and staff are heard in the gap analysis because of the proliferation of personally-owned mobile devices and the specific needs and preferences of those users. When describing the ideal framework for a gap analysis, Douglas stated:

> So, let's say you're a small two-year or four-year institution, let's say 10,000 students or less. We would go in two days on site. We would meet half a day with the IT side of the house, get the sense for the controls, and a day and a half meeting with registrar's office and foundation and faculty and really get a sense for where's the gap. And these days, with things moving in the cloud with software as a service and with BYOD, these types of gap analyses are usually critical. (Everett Douglas, Interview, 2015, 1/04:16)

There is a strong likelihood that the IT department does not even know all of the ways that faculty and staff are using mobile devices to perform their work. Douglas suggested that hiring an outside consultant to do this work may yield a more objective result

(Everett Douglas, Interview, 2015). Afterwards, it is important that the gap analysis be utilized and implemented and not just stuck on a shelf. It should form the basis of a security program or roadmap for the institution to follow to make their environment more secure.

Employ a data classification guideline or policy.

An important part of securing mobile devices is being able to tell the end users what they can and cannot do with their mobile devices. What data can they download to their devices? What systems can they log into with their devices? Before an institution can train end users, they need to know the answer to the data classification question. Friedman and Hoffman (2008) state that "Security policies must be defined, documented and published to end users before they can be enforced" (p.18). Brooks stated that:

> The people are the weakest link, in my opinion, more often than not, with social engineering stuff and bad data management practices that are really hard to defend against. (Duncan Brooks, Interview, 2015, 16:21)

Once an institution knows what types of data they are dealing with, they can begin to educate their users on what they can and cannot do with data, and whether or not they can access it from their mobile device.

The data classification policy provides the entire framework for what data institutions have to protect and what data they do not have to protect. It is one of the critical foundational pieces to any security program (Mahesh & Hooter, 2013; French, Guo, & Shim, 2014; Joel, 2010; Friedman and Hoffman, 2008). For example, picture a staff member in the health center has an iPad. The data classification policy states that regular University data are unprotected but that any student health record data are in a

"restricted" class. "Restricted" means that it can only be accessed from specific designated computers on-campus only. Having been informed of the policy, each staff member now knows that she cannot access the health records data from her personal iPad device. Without this policy, it becomes incredibly difficult to train end users, the biggest risk vector, on what they can and cannot do. The data classification policy is not a static item and should be reviewed on a yearly basis. As new technologies are introduced and new types of data, this policy needs to grow to provide guidance to the end users on how to best secure that new data.

Implement a security awareness program.

A security awareness program is another foundational item. The literature review indicated that end users are the number one biggest risk (Friedman & Hoffman, 2008; Educause, 2011), and interview subjects suggested that every institution should have a security awareness plan to assist in combatting this problem. Gregory stated:

> One of the pillars of a robust security program is understanding how much training is necessary. We are embarking on a pretty ambitious plan to start corralling our users and giving them the right level of training, part of which is understanding mobile security issues. (Michael Gregory, Interview, 2015, 32:05)

It may be best to start out small with just some training on a particular topic, such as password security, or the focus can be on one particular risk area, such as HIPPAA compliance. In a perfect world, the gap analysis should indicate where to start, but institutions do not have to wait for that. Start small, get the campus community involved, and build off evolving success and momentum to grow the security awareness program as you develop the over-arching security program.

In order to be successful, the security awareness program needs to be well-planned, to have goals, and to be positive in tone. Once fully up and running, the security awareness program should not be a stand-alone onetime initiative, although it may start out that way before all the pieces of the security plan are aligned. In order to be truly successful, it should be a long-term plan for on-going and consistent communications. Security around mobile devices should be one component and should wrap into an over-arching security awareness plan that integrates into the over-arching security plan for the entire institution. Doing this ensures that the message about mobile device security is consistent throughout.

Adamson believes that vetting the strategy for security should be part of the larger campus security awareness plan. He stated that:

> It's part of security awareness, in my opinion. The more I can make people aware of security, and it has to be relevant to them. I have to be able to explain it in a way that this is how it impacts them. If I just say, "Change your password." "Well, why do I have to change my password? I like my password." But if I say, "You need to change your password because it's good practice, and we've been breached X,Y,Z." If I can tell them how it impacts them, they're much more likely to be able to do that and understand why I'm asking them to do something. (Kurt Adamson, Interview, 2015, 16:38)

A critical component to think about before implementing a security awareness program should be assessment. Prior to implementing, it is critical to develop the indicators of success and a method of assessing that. If an institution skips this step, there will be no data to determine if the security awareness program is successful or not.

Because a security awareness program takes resources, both financial and staff time, institutions will want to know if the cost is producing enough benefit to make the investment worthwhile and if the security awareness program needs to be changed in order to become more successful.

Move the conversation up a level, and make sure it's the *right* conversation.

Too often, security conversations are happening within IT, but not anywhere else. The conversation needs to happen at a higher level than IT alone, and it needs to be in the right language. The conversation should not be a technical conversation, but needs to be tailored to what administrators in particular need to know. This was not something present in literature reviewed, but it was a theme that arose from the interviews. Douglas stated that trend data today shows that:

> There's a thirst for more cyber risk discussions. Obviously, mobile devices with the BYOD, it's a big worry and topic these days. (Everett Douglas, Interview, 2016, 1/00:40)

Because security at higher education institutions impacts faculty, staff, and students, it is important that the leaders in these areas be involved. Roles such as the Provost, Deans, Student Affairs, and many others need to be aware of and have a chance to contribute to the conversation around creating the right balance of security and access to data and systems. When discussing how to start working on a security plan, Adamson states:

> I have to discuss it with any number of different people, with our IT administrative staff, and I'll speak with the University administration, the rest of the IT staff, working staff. Most of the stuff that comes out of information

> security is work for other people. So I have to be aware of that and how that impacts their workload. (Kurt Adamson, Interview, 2015, 15:46)

However, keep in mind that the right conversations need to happen at the right level. Douglas stated that:

> It's not just on the CIO, CISO side of the house, on the technical side of the house, but making sure that you provide a perspective and information that's consumable to folks even higher up. (Everett Douglas, Interview, 2015, 1/00:06)

More in-depth risk conversations can still happen within IT, but the information that flows to upper administration needs to be brief, clean, and easy to convey for the management team to be able to understand, digest, give feedback on, and make decisions about the security initiatives at hand.

Grow all IT professionals in security skills, not just identified security professionals.

The topic of IT security is broad and vast. Implementing security measures can take a great deal of resources, and many institutions do not have sufficient staff lines to devote solely to this topic. It must be pervasive through every part of IT from the front-line help desk staff to the back-end systems staff in order to be consistent and successful. Security should be a part of every IT person's job. Invest in all IT staff participating in security training and learning about how security impacts their specific IT jobs and the institution as a whole. It cannot be a one-person job, even at small institutions. Security is everyone's business.

Hudson stated that rather than investing more resources internally in the security team at central IT, he would prefer resources to instill security into the mindset of IT

professionals across the entire institution, both through educating them and helping them care about security on a regular basis (Matthew Hudson, Interview, 2015). Investing and growing the entire IT staff in the field of security as it relates to their positions will create a consistent, cohesive IT department that is security-conscious regardless of the topic at hand.

Connect with leaders in other venues.

The complexity of the topic of IT security can cause leaders to feel overwhelmed. However, when one looks at all the components that need to be addressed, it is important to remember that leaders are not alone. Other IT and campus leaders out there are struggling with these same issues. Many of the interview subjects cited problems such as too few resources, uncertainty around which security risks to take on first, and what strategies work best. Do not struggle alone with these questions. Connecting with a network of peers who are struggling with these same questions around mobile device security can help the institution adopt a strategy that is much more well-rounded than one person thinking and acting alone. REN-ISAC was a frequently brought up example of such a community (Victor Samuels, Interview, 2015; Michael Gregory, Interview, 2015; Everett Douglas, Interview 2015).

Recommendations for Further Research

Research demonstrates that mobile device security is a growing field. Friedman and Hoffman (2008) state that:

> This evolution toward a predominately mobile workforce is being driven by lifestyle choices, productivity gains, and technology improvements. Workers are demanding the flexibility of staying at home on some workdays, as well as

> working at home during evenings and weekends. Businesses are seeing major productivity benefits by keeping workers fully functional on the road and at customer sites. Wide-spread adoption of Wi-Fi and 3G mobile data networking technologies have facilitated global information sharing. Rapid innovation in the form and usability of mobile devices has opened fresh horizons for new types of mobile applications. (p. 159)

While this research provided a glimpse into what some institutions are doing regarding mobile device security, the field of mobile device security is changing at a rapid pace. While a few years ago, trends were pushing to secure the devices, trends now are directing institutions to secure the data and worry less about the devices themselves. It is important that research continues to examine the greatest security risks as things continue to evolve in the future. Looking toward business is a good way to keep ahead of this, as typically higher education IT departments lag slightly behind business IT departments in terms of the rate of adoption of new trends and technologies.

Further research is needed to understand the changing dynamics of the usage of mobile devices for education as well. Today, many of the institutions studied are doing little with regard to using mobile devices in the classroom, but there is evidence that this is beginning to shift as students coming up through the K-12 system are using iPads in their classes on a daily basis and bringing that mindset into higher education institutions as they enter. Because of this, future research should examine what, specifically, students and faculty are doing in the classrooms with these mobile devices and seek to explore the security risks of those tasks and actions. In addition, future research should examine how many faculty, staff, and students are currently protecting their devices with passcodes and

should compare the rate of passcode adoption between the faculty/staff population and the student population.

While research indicates that institutions should focus on protecting the data at the core, there are limitless ways of doing that. Further study is needed to determine the appropriate methods to secure the data, and it is likely unique to each type of data source that an institution possesses. Studies could be done for each type of operating system (Android versus iOS), about each system (e-mail, file storage, internal databases, et cetera), about each type of security measure (passcodes, firewalls, et cetera), or about how to secure specific types of populations (guests, students, faculty, et cetera.) This is an expansive problem and one that requires further in-depth examination. It is clear because of the complexity of this issue that answering the question "how do we secure our data?" would need to be broken down into manageable smaller research components in order to be successful.

Additional research would also be helpful to study the resources and networks that are available for leaders to learn about IT security issues. Research uncovered that each state and region had their own networks, their own associations, their own microcosms of people that gathered together to discuss security issues. As new CIOs and higher education leaders enter the field, it can be difficult to discover these resources. Research that pointed new and emerging leaders towards the key memberships to join, conferences for which to sign up, and trainings to attend would be extremely helpful in getting those leaders started off on the right foot.

The body of literature would also be broadened in the future by studies around what types of breaches have occurred in higher education settings. This research should

examine why the breach occurred, what was done to respond to the breach, and what is being done to prevent future breaches from occurring.

Future research could also include studying what it takes to make a successful CISO. It was clear in the interviews that some CISOs are more successful in their role than others. Many higher education institutions are at the precipice of hiring this critical role. Some of them are looking internally towards networking or other IT staff, and that is not always a successful transition. The interviews above suggest a better fit is actually someone with a business background. However, further research would be beneficial to determine the right mix of skills to look for when hiring this role. A study that answers the question “What should I look for when hiring a successful CISO?” would have a great deal of value in higher education in the coming years as more institutions hire this position.

Conclusion

In conclusion, this research study illustrates that many institutions are still in the infant stages of securing mobile devices. However, because mobile devices are not largely targeted for massive data breaches today, institutions have time to develop a strategy around mitigating the risks presented by these devices entering the higher education environment. Though the security risk itself is great, hackers and others with malicious intent are also in their infancy with regard to mobile devices. Because of this, it is critical that higher education institutions make security of these devices a prominent part of their strategic plan in order to be prepared for the future.

Advancements in cloud technologies are making the devices less and less important and protecting the data more and more important. In adopting a future-oriented

strategy, institutions should focus on protecting the data being accessed, not the device itself.

Furthermore, the security of mobile devices needs to be embedded within the institution and not isolated to just the responsibility of the IT department. While institutions should hire a CISO, or someone in a full-time IT security role, to take charge of creating and implementing the strategic plan around IT security, it should not be this person's job alone. Only through partnerships between IT and the rest of the institution will improvements in security be made. The security of mobile devices is the job of everyone at the institution.

REFERENCES

Agee, A. S., Yang, C., & Educause Current Issues Committee. (July/August 2009). Top Ten IT Issues 2009. *Educause Review*, 45-58.

Allison, D. H., DeBlois, P. B., & Educause Current Issues Committee. (2008). Current Issues Survey Report, 2008. *Educause Quarterly, 2*, 14-30.

Baker, W. H. & Wallace, L. (2007). Is information security under control? *IEE Computer Society*, 36-44.

Baltimore County Public Schools. (2010). Research Process Steps. Retrieved from https://www.bcps.org/offices/lis/researchcourse/develop_writing_methodology_limitations.html

Boes, R., Cramer, F. T., Dean, V., Hanson, R., & McKenna, M. N. (2006). Campus IT Security: Governance, strategy, policy, and enforcement. *Educause Center for Applied Research Bulletin, 17*, 1-13.

Botha, R. A., Furnell, S. M., & Clarke, N. L. (2009). From desktop to mobile: Examining the security experience. *Computers & Security, 28*(3-4), 130-137. doi:DOI: 10.1016/j.cose.2008.11.001

Brechbuhl, H., Bruce, R., Dynes, S., & Johnson, M. E. (2010). Protecting critical information infrastructure: Developing cybersecurity policy. *Information Technology for Development, 16*(1), 83-91. doi:10.1002/itdj.20096

Camp, J. S., DeBlois, P. B, & Educause Current Issues Committee. (2007). Current Issues Survey Report, 2007. *Educause Quarterly, 2*, 12-31.

CDW-G Federal Cybersecurity Report: Danger on the Front Lines. (2009). CDW Government, Inc., 1-27.

Cheng, J. (2007). *Collaborative network security for heterogeneous mobile networks.* University of California. *ProQuest Dissertations and Theses.*

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones – A survey of attitudes and practices. *Computers & Security, 24*(7), 519-527. DOI: 10.1016/j.cose.2005.08.003

Creswell, J. W. (2008). *Educational research. Planning, conducting, and evaluating quantitative and qualitative research* (3rd ed.). Upper Saddle River, NJ: Merrill/Prentice Hall.

Custer, W. L. (2010). Information security issues in higher education and institutional research. *New Directions for Institutional Research, 146,* 23-49.

Educause. (March 2011). 7 Things You Should Know about Mobile Security. Retrieved from http://www.educause.edu/ir/library/pdf/EST1101.pdf

Educause. (August 2014). Foundations of Information Security: Institutional Implications of Safeguarding Data. Retrieved from http://net.educause.edu/ir/library/pdf/pub4011.pdf

Elahi, H., & Islam, S. (2014). *Go fast, go with mobile: Student perception on implementing mobile based library services at Dhaka University Library* (Doctoral dissertation). Library and Information Science Commons. (Paper 1197).

Enany, A. (2007). *Achieving Security in Messaging and Personal Content in Symbian Phones*. Blekinge Tekniska Högskola/Sektionen för Teknik (TEK).

Ericsson Press. (2010). Mobile Data Traffic Surpasses Voice. Retrieved from http://www.ericsson.com/thecompany/press/releases/2010/03/1396928

French, A. M., Guo, C, & Shim, J. P. (2014) Current Status, Issues, and Future of Bring Your Own Device (BYOD). *Communications of the Association for Information Systems, 35*(10), 191-197.

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management, 7*(1), 159-180.

Fuller, M. J. (2014). *Click to agree: Policies impacting a one-to-one mobile learning environment* (Doctoral dissertation). National Louis University. (Paper 77). Retrieved from http://digitalcommons.nl.edu/diss/77

Goasduff, L. (Interviewer) & Zumerle, D (Interviewee). (2015). *Mobile Security Threats and Trends 2015* [Interview transcript]. Retrieved from Gartner web site: http://www.gartner.com/newsroom/id/3127418

Grajek, S., & 2012-2013 Educause IT Issues Panel. (May/June 2013). Welcome to the Connected Age: Top Ten IT Issues 2013. *Educause Review,* 31-57.

Grajek, S., & 2013-2014 Educause IT Issues Panel. (March/April 2014). Top Ten IT Issues, 2014: Be the change you see. *Educause Review,* 10-46.

Grajek, S., & 2014-2015 Educause IT Issues Panel. (January/February 2015). Top Ten IT Issues, 2015: Inflection point. *Educause Review,* 10-48.

Higher Education Believes Networks are More Secure Now. (2009). *Worldwide Videotex, 10* (7), 1-3.

Imgraben, J., Engelbrecht, A., & Choo, K. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users.

Behaviour & Information Technology, *33*(12), 1347-1360. doi: 10.1080/0144929X.2014.934286

Ingerman, B. L., Yang, C., & Educause Current Issues Committee. (May/June 2010). Top Ten IT Issues 2010. *Educause Review*, 46-60.

Joel, A. W. (2010). Choosing both: Making technology choices at the intersections of privacy and security. *Texas Law Review, 88*(7), 1751-1765.

La Polla, M., Martinelli, F., & Sgandurra, D. (2012). A Survey on Security for Mobile Devices. *IEEE Communications Surveys & Tutorials, 15*(1), 446-471. doi: 10.1109/SURV.2012.013012.00028

Mahesh, S. & Hooter, A. (2013). Managing and Securing Business Networks in the Smartphone Era. *Management Faculty Publications*. (Paper 5). Retrieved from http://scholarworks.uno.edu/mgmt_facpubs/5

McElroy, L. & Weakland, E. (2013). Measuring the Effectiveness of Security Awareness Programs. *Educause Center for Analysis and Research: Research Bulletin,* 1-10.

Merriam, S.B. (2009). *Qualitative Research: A guide to design and implementation.* San Francisco, CA: Jossey-Bass.

Miller, K., Voas, J., & Hurlburt, G. (2012). BYOD: Security and Privacy Considerations. *IT Professional, 14*(5), 53-55.

NYSE Governance Services & Vericode. (2015). Cybersecurity in the Boardroom. Retrieved from https://www.veracode.com/sites/default/files/Resources/Whitepapers/cybersecurity-in-the-boardroom-whitepaper.pdf

Ongtang, M. (2010). *Securing mobile phones in the evolving mobile ecosystem.* The Pennsylvania State University. *ProQuest Dissertations and Theses.*

Thomson, G. (2012). BYOD: Enabling the chaos. *Network Security, 2012*(2), 5-8. doi:http://dx.doi.org/10.1016/S1353-4858(12)70013-2

Turner, R. (2011). A new focus for IT security? *Computer Fraud & Security, 2011*(2), 7-11. doi:10.1016/S1361-3723(11)70016-1

United States Department of Education. (2011). The Database of Accredited Postsecondary Institutions and Programs. Retrieved from http://ope.ed.gov/accreditation/

Verma, I. (2011). *A security analysis of smartphones*. Purdue University Graduate School.

Wang, P. (2007). *Securing communication in dynamic network environments.* North Carolina State University). *ProQuest Dissertations and Theses.*

Wankel, L. & Blessinger, P. (2012). New Vistas in Higher Education: An Introduction to Using Social Technologies. *Cutting-edge Technologies in Higher Education*, 3-16. http://dx.doi.org/10.1108/s2044-9968(2012)000006b003

Wheatman, J. (2010). Four hot issues from Def Con 18: Traditional threats remain, but new problems come to the fore. *Gartner, Inc.*

Yoon, M. (2008). *Securing computer networks: Access control management and attack source identification.* University of Florida. *ProQuest Dissertations and Theses.*

APPENDIX

Appendix A

IRB Approval Letter

From: IRB NUgrant System [nugrant-irb@unl.edu]
Sent: Thursday, June 25, 2015 1:39 PM
To: Bryant, Miles; Gordon, Casey J
Subject: NUgrant Message - Official Approval Letter for IRB project #15230

June 25, 2015

Casey Gordon
Department of Educational Administration

Miles Bryant
Department of Educational Administration
133 TEAC, UNL, 68588-0360

IRB Number: 20150415230 EX
Project ID: 15230
Project Title: Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know

Dear Casey:

This letter is to officially notify you of the certification of exemption of your project by the Institutional Review Board (IRB) for the Protection of Human Subjects. Your proposal is in compliance with this institution's Federal Wide Assurance 00002258 and the DHHS Regulations for the Protection of Human Subjects (45 CFR 46) and has been classified as Exempt Category 2.

You are authorized to implement this study as of the Date of Exemption Determination: 04/01/2015.

1. Your stamped and approved informed consent document has been uploaded to NUgrant (files with Approved.pdf in the file name). Please use this document to distribute to participants. If you need to make changes to the informed consent document, please submit the revised document to the IRB for review and approval prior to using it.

2. You may recruit participants from the following institutions:

We wish to remind you that the principal investigator is responsible for reporting to this Board any of the following events within 48 hours of the event:
* Any serious event (including on-site and off-site adverse events, injuries, side effects, deaths, or other problems) which in the opinion of the local investigator

was unanticipated, involved risk to subjects or others, and was possibly related to the research procedures;
* Any serious accidental or unintentional change to the IRB-approved protocol that involves risk or has the potential to recur;
* Any publication in the literature, safety monitoring report, interim result or other finding that indicates an unexpected change to the risk/benefit ratio of the research;
* Any breach in confidentiality or compromise in data privacy related to the subject or others; or
* Any complaint of a subject that indicates an unanticipated risk or that cannot be resolved by the research staff.

This project should be conducted in full accordance with all applicable sections of the IRB Guidelines and you should notify the IRB immediately of any proposed changes that may affect the exempt status of your research project. You should report any unanticipated problems involving risks to the participants or others to the Board.

If you have any questions, please contact the IRB office at 472-6965.

Sincerely,

Becky R. Freeman, CIP
for the IRB

Appendix B

Script for Initial Phone Contact with Institution

Hello. My name is Casey Gordon, and I am a student at the University of Nebraska Lincoln. I am calling to ask for your institution's participation in a research study I am conducting about mobile devices and the security of these devices in higher education institutions.

Participation would include a minimum of four individuals involved with mobile devices and security at your institution. I would ask each of these individuals to participate in a 30 to 60 minute phone interview about their experiences with mobile device security, with the possibility of additional follow-up interviews.

This research study will assist higher education institutions in providing improved support for the security of mobile devices used by their faculty and staff. If you do not wish to participate in this study, there will be no negative repercussions to you or your institution.

Is this something you would be willing to allow your institution to participate in?

Appendix C

Script for Initial Phone Contact with Individual Participants

Hello. My name is Casey Gordon, and I am a student at the University of Nebraska Lincoln. I am calling to ask for your participation in a research study I am conducting about mobile devices and the security of these devices in higher education institutions.

Your institution has already agreed to let me conduct this research on your campus and <insert contact person's name> gave me your name as a possible interview subject because of your expertise with mobile devices and security.

Participation would involve a 30 to 60 minute in-person interview about this topic, where you would be asked about your experience with mobile devices at <insert institution name here> and how your institution is addressing security issues on these devices. There is a possibility of an additional follow-up interview, if needed.

This research study will assist higher education institutions in providing improved support for the security of mobile devices used by their faculty and staff. If you do not wish to participate in this study, there will be no negative repercussions to you or your institution.

Are you willing to participate in this research study?

Appendix D

Script for Initial E-mail Contact with Individual Participants

Dear <insert recipient's first name>,

Your institution has agreed to let me conduct a research study about mobile device security on your campus, and I am writing to ask for your participation in a 30 to 60 minute phone interview about this topic, with the possibility of a 30 minute follow-up interview. You will be asked questions about your experience with mobile devices at <insert institution name here> and how your institution is addressing security issues on these devices. Both you and your institution will remain anonymous in the final study. This research study will assist higher education institutions in providing improved support for the security of mobile devices used by their faculty and staff.

Your assistance with this research study is greatly appreciated, but if you are not willing to participate, there will be no negative repercussions to you or your institution. If you have any questions, please contact me at XXXXXX@XXXXXXXXXXX or call me at XXX-XXX-XXXX. Thank you in advance for your willingness to share your experiences.

Thank you,

Casey Gordon
Educational Administration Ph.D. Candidate
University of Nebraska Lincoln

Appendix E

Interview Informed Consent Form for Individual Participants

University of Nebraska Lincoln

COLLEGE OF EDUCATION AND HUMAN SCIENCES
Department of Educational Administration

INFORMED CONSENT FORM

Identification of Project:

Assessing Security Risks for Mobile Devices: What Higher Education Leaders Should Know

Purpose of the Research:

The purpose of this research study is to assist higher education leaders in preparing their institutions to handle mobile device security for their faculty, staff, and administrator populations. This study seeks to determine the security issues around mobile devices that are facing higher education institutions and how the leaders of those higher education institutions can prepare their institutions to handle these issues. In addition, this study seeks to answer the question as to how leaders can continue to address mobile device security issues in ways that are sustainable into the future.

Procedures:

Participation in this study is completely voluntary. We would like to conduct a 60 to 90 minute phone interview with you about your experience with mobile device security at your institution. Also, if necessary, you may be asked to participate in an additional phone interview to clarify and provide additional details, not to exceed 1 hour in length. These interviews will be audio taped with your permission. You are being chosen to participate based on your role in security issues at a higher education institution.

Risks and/or Discomforts:

There are no known risks or discomforts associated with this research. However, because this research will be made available to the public, we ask that you share only public information and no confidential information.

Benefits:

The benefits of this research study are that it will assist higher education leaders in determining how to address and potentially prevent the security risks of mobile devices in their own institutions.

Confidentiality:

Your institution will not be named in the final study. However, any information obtained during this study which could identify you will be kept strictly confidential. The data will be stored in a locked cabinet in the investigator's office and will only be seen by the investigator during the study and for five years after the study is complete. The information obtained in this study may be published in scientific journals or presented at scientific meetings but the data will be reported as aggregated data. The audiotapes will also be stored in a locked file cabinet.

Compensation:

There will be no compensation for participating in this research.

Opportunity to Ask Questions:

You may call the investigator at any time at [redacted] If you have questions concerning your rights as a research subject that have not been answered by the investigator or to report any concerns about the study, you may contact the University of Nebraska-Lincoln Institutional Review Board, telephone (402) 472-6965.

Freedom to Withdraw:

You are free to decide not to participate in this study or to withdraw at any time without adversely affecting your relationship with the investigators, the University of Nebraska or your institution. Your decision will not result in any loss or benefits to which you are otherwise entitled.

Consent, Right to Receive a Copy:

You are voluntarily making a decision whether or not to participate in this research study. Your signature certifies that you have decided to participate having read and understood the information presented. You will be given a copy of this consent form to keep.

_____ Check if you agree to be audio taped during the interview.

Signature of Participant:

_____ _____

Signature of Research Participant *Date*

Name and Phone number of investigator(s)

Casey J. Gordon, Ph.D. Candidate, Principal Investigator
Miles Bryant, Ph.D., Secondary Investigator

[redacted]

Appendix F

Interview Protocol

Sub-questions (a, b, et cetera) are optional prompts if needed to encourage conversation.

1. Please tell me about your position and role at the institution.
    a. What position do you hold?
    b. How long have you worked in this position?
2. Please describe the role you take in working with mobile devices and/or security at your institution.
3. What policies and procedures does your institution have regarding the topic of mobile devices and security of those devices?
    a. What drove you to develop these particular policies?
    b. How does your institution implement and enforce these policies?
4. What types of systems do you use to manage mobile devices (example: Mobile Device Management solution (MDM) or something similar)?
5. What information does your institution collect about mobile devices and usage by faculty, staff, and/or students?
    a. How did you decide what to collect and what not to collect?
    b. If so, what information do you collect about University-owned devices versus personal-owned devices?
    c. If so, what information do you collect regarding how these devices are used, what apps are being purchased, what features are most utilized, et cetera?
    d. For what, if anything, does your institution utilize this data?
6. Describe an incident or issue regarding mobile device security that your institution has faced recently.

7. What trends do you see coming in the future regarding mobile devices and/or security?
    a. Where do you gather data about mobile device security?
8. What do you think your institution does well regarding the security of mobile devices?
9. What do you think your institution does regarding the security of mobile devices that needs improvement?
10. What do you think the perception is of the security of mobile devices by the faculty and staff?
11. What resources, processes, policies, et cetera do you wish your institution had to assist with the security of mobile devices?

Appendix G

Confidentiality Form for Transcription Service

CONFIDENTIALITY FORM

Identification of Project:

Addressing Security Risks for Mobile Devices: What Higher Education Leaders Should Know

Purpose of the Research:

The purpose of this research study is to assist higher education leaders in preparing their institutions to handle mobile device security for their faculty, staff, and administrator populations. This study seeks to determine the security issues around mobile devices that are facing higher education institutions and how the leaders of those higher education institutions can prepare their institutions to handle these issues. In addition, this study seeks to answer the question as to how leaders can continue to address mobile device security issues in ways that are sustainable into the future.

Procedures:

The investigator will submit approximately 16-24 interview tapes to the transcription service for verbatim transcription.

Confidentiality:

Any information shared with the transcription service will be kept strictly confidential. The data will be stored securely at the transcription service location and will only be seen by the transcriber during transcription. Upon completion of the transcription process, all data will be returned to the researcher. No records will be retained by the transcription service.

Opportunity to Ask Questions:

You may call the investigator at any time at (XXX) XXX-XXXX. If you have questions concerning your rights as a research subject that have not been answered by the investigator or to report any concerns about the study, you may contact the University of Nebraska-Lincoln Institutional Review Board, telephone (402) 472-6965.

_____ _____

Signature *Date*

Name and Phone number of investigator(s)

Casey J. Gordon, Graduate Student, Principal Investigator
Miles Bryant, Ph.D., Secondary Investigator